ISO/IEC JTC 1
Information technology
Secretariat: ANSI (United States)

Document type: Business Plan

Title: SC 27 Business Plan October 2013 – September 2014

Status: This document is circulated for review and consideration at the November 2013 JTC 1 Plenary meeting in France.

Date of document: 2013-09-30

Source: SC 27 Chairman

Expected action: ACT

Action due date: 2013-11-04

Email of secretary: lrajchel@ansi.org

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1

ISO/IEC JTC 1/SC 27 N12830

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 2013 – September 2014

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2013-09-30

PROJECT:

STATUS: for submission to JTC 1

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
H. Cuschieri, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
T. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

MEDIUM: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

NO. OF PAGES: 1 + 15

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787, [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-4-2652; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

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

Period covered: October 2013 – September 2014

Submitted by: Walter Fumy, SC 27 Chairman

1 Management Summary

1.1 Chairman's Remarks

This Business Plan has been prepared in accordance with Resolution 52 of the 25th SC 27 Plenary meeting in Sophia Antipolis, France, 29th - 30th April 2013. .

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 206
- number of active projects 79
- number of publications: 127

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 projects have been approved over the past 12 months either via 3-month NP ballot, 60-day letter ballot, or by subdivision of existing projects. All of the new projects are supported by substantial NB interest:

- ISO/IEC NP 11770-6: *Key management -- Part 6: Key derivation*
- ISO/IEC NP TR 19249: *Catalogue of architectural and design principles for secure products, systems, and applications*
- ISO/IEC NP 20009-4: *Anonymous entity authentication -- Part 4: Mechanisms based on weak secrets*
- ISO/IEC NP 27009: *The use and application of ISO/IEC 27001 for sector/service-specific Third-Party accredited certifications*
- ISO/IEC NP 27050: *Electronic discovery*
- ISO/IEC NP 29151: *Code of practice for the protection of personally identifiable information*
- ISO/IEC 29192-4/Amd.1: *Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques – Amendment 1*
- ISO/IEC NP 29192-5: *Lightweight cryptography -- Part 5: Hash-functions*

In addition, SC 27 has resolved to revise the following projects:

ISO/IEC 10116: *Modes of operation for an n-bit block cipher* (3rd ed. 2006-02-01)

- ISO/IEC 14888-3: *Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms* (2nd ed. 2006-11-15)
- ISO/IEC 18032: *Prime number generation* (1st ed. 2005-01-15)
- ISO/IEC TR 19791: *Security assessment of operational systems* (2nd ed. 2010-04-01)
- ISO/IEC 27005: *Information security risk management* (2nd ed. 2011-06-01)
- ITU-T Recommendation X.1051 I 27011: *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002* (1st edition 2008-12-15)

- ISO/IEC 27013: *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1* (1st ed. 2012-10-15)

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

- SC 27 study period on Cloud computing security and privacy
- SC 27 study group on Framework for PKI Policy / Practices / Audit (SG-PKI)
- Future version development of ISO/IEC 27000 (WG 1)
- Homomorphic encryption schemes (WG 2)
- Secret sharing (WG 2)
- Broadcast encryption (WG 2)
- Cryptographic mechanism conformance testing (WG 2)
- Revision of ISO/IEC 10118-3 (WG 2)
- Predictive assurance (WG 3)
- High-assurance evaluation under ISO/IEC 15408/18045 (WG 3)
- Security evaluation of anti-spoofing techniques for biometrics (WG 3/WG 5)
- Standards for privacy seal programs (WG 3/WG 5)
- Cloud security technology standards (WG 4)
- Coordination of investigative projects (WG 4)
- Documentation of data deletion principles for personally identifiable information in organizations (WG 5)
- Privacy impact assessment (WG 5)

1.4 Co-operation and Competition

SC 27 enjoys an extremely large number of productive and valuable liaisons with many organizations within ISO/IEC JTC 1 including WG 6, WG 7, SC 6, SC 7, SC 17, SC 25, SC 31, SC 36, SC 37 and SC 38, within ISO including TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, ISO/CASCO, TMB/JTCG MSS, TMB/SAG, within IEC including IEC/TC 57, IEC/TC 65, and to external organizations including ABC4Trust, ARTICLE 29 Data Protection Working Party, CCDB, CDFS, CEN/TC 377, CEN/CENLEC/ETSI/SGCG Smart Grid Coordination Group, CSA, ENISA, EPC, ETSI, EuroCloud, FIDIS, FIRST, ICDPPC, INLAC, INTERPOL, ISACA, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, PICOS, TCG and VISA.

Currently SC 27 maintains 25 internal and 32 external liaisons. A complete list is available at www.jtc1sc27.din.de/sbe/members .

Selected aspects related to these liaisons are highlighted below.

1.4.1 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'.

1.4.2 TC 68/SC 2 'Financial Services - Security'

TC 68/SC 2 and SC 27 coordinate on IT security standards of mutual interest by sharing expertise and content, in order to avoid potential overlap in IT security standards development. SC 27 is looking forward to further coordinate with the recently established new TC 68/SC 2 Management Team.

1.4.3 ITU-T Q3/SG17 and ITU-T FG Cloud Computing

ITU-T Q3/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

- Recommendation ITU-T X.841 I ISO/IEC 15816: *Security information objects for access control*
- Recommendation ITU-T X.842 I ISO/IEC TR 14516: *Guidelines on the use and management of Trusted Third Party services*
- Recommendation ITU-T X.843 I ISO/IEC 15945: *Specification of TTP services to support the application of digital signatures*
- Recommendation ITU-T X.1051 I ISO/IEC 27011: *Information security management guidelines for telecommunications* Recommendation ITU-T X.1054 I ISO/IEC 27014: *Governance of information security*
- Recommendation ITU-T X.1254 I ISO/IEC 29115: *Entity authentication assurance*
- Draft Recommendation ITU-T X.1085 (bhsm) I ISO/IEC 17922: *Telebiometric authentication framework using biometric hardware security module*

.

1.4.4 The Common Criteria Development Board (CCDB)

The CCDB 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 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 CCDB to review, comment and contribute to the project. Both the ISO/IEC 15408 and ISO/IEC 18045 are currently fully aligned with their CCDB counterparts. Recently the WG has been contributing to the CCDB exploratory work on future development of Common Criteria.

A number of SC 27/WG 3 projects complement the application of ISO/IEC 15408, such as ISO/IEC TR 20004 *Refining Software Vulnerability Analysis under ISO/IEC 15408 and ISO/IEC 18045*, or ISO/IEC 17825 *Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules*. This extended coverage increases the collaboration with the CCDB.

1.4.5 The Trusted Computing Group (TCG)

ISO/IEC 11889: *Trusted Platform Module* is the main area of common interest, as the TCG with PAS submitter status, is interested in its further maintenance. The TCG has submitted their draft specifications of the TPM 2.0, and they have been subject to comment and discussion by SC 27/WG 3 NBs, experts and TCG liaison officers.

In view of the experience with this cooperation, SC 27 has requested JTC 1 to remove assignment of projects from the SC 27 Programme of Work, for which the maintenance remains with the PAS submitter.

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 the financial industry - and 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 (remote) 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 accredited 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 the privacy of their information and 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. relating to the issue, who controls and is entitled to use which very personal data about whom. SC 27 addresses the technological challenges resulting from 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- and m-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. ISO/IEC 27014 Governance of information security will define a framework, establish objectives, principles, and processes, and show how it can be used to evaluate, direct, and monitor an information security management system. SC 27 is also working closely with JTC 1/SC 7 in the development of ISO/IEC 30121, Governance of digital forensic risk framework.

Furthermore, the so-called "Internet of things" is gaining more and more attention. Technologies such as RFID pose new challenges with respect to security and privacy, and in view of specific constraints, require dedicated solutions, such as lightweight cryptographic techniques, authentication, etc.

For seamless security across devices and applications, ISO/IEC 11889 Trusted Platform Module has been specified and included into the SC 27 work programme.

More and more, organizations are recognizing the importance of addressing security within systems and software engineering processes, as well as within the supply chain.

Apart from the need for guidelines and standards enabling or contributing to the implementation and assurance of security, a need exists for guidelines and standards addressing incident management, specific activities in handling potential digital evidence, and common investigation processes across various investigation scenarios.

2.2 Achievements

2.2.1 Publications

Since October 2012, the following International Standards and Technical Reports have been published:

- ISO/IEC TR 15443-1: *Security assurance framework -- Part 1: Introduction and concepts* (2nd ed.)

  Publication date: 2012-11-15 – 51 pages

  ISO/IEC TR 15443-1:2012 defines terms and establishes an extensive and organized set of concepts and their relationships for understanding IT security assurance, thereby establishing a basis for shared understanding of the concepts and principles fundamental to ISO/IEC TR 15443 across its user communities.

- ISO/IEC TR 15443-2: *Security assurance framework -- Part 2: Analysis* (2nd ed.)

  Publication date: 2012-11-15 – 18 pages

  ISO/IEC TR 15443-2:2012 builds on the concepts presented in ISO/IEC TR 15443-1. It provides a discussion of the attributes of security assurance conformity assessment (SACA) methods that contribute towards making assurance claims and providing assurance evidence to fulfil meeting the assurance requirements for a deliverable. ISO/IEC TR 15443-2 proposes criteria for comparing and analyzing different SACA methods. The methods used as examples in ISO/IEC TR 15443-2 represent popularly used methods at the time of its writing. New methods may appear, and modification or withdrawal of the methods cited may occur. It is intended that the criteria can be used to describe and compare any SACA method whatever its provenance.

- ISO/IEC 20009-1: *Anonymous entity authentication -- Part 1: General (1st edition)*

  Publication date: 2013-08-01 – 6 pages

Anonymous authenticated communication hides the identifier of an authenticated entity to its communicating partner and/or to a third party, while retaining the property that a verifier can reliably determine that its communication partner is authentic, i.e. that it possesses certain attributes, e.g. membership of a predefined group of entities. ISO/IEC 20009-1:2013 specifies a model, requirements and constraints for anonymous entity authentication mechanisms.

- ISO/IEC 27000: *Information security management systems – Overview and vocabulary* (2nd ed.)

  Publication date: 2013-01-14 – 25 pages

  ISO/IEC 27000:2012 describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions. ISO/IEC 27000 is applicable to all types and sizes of organizations (e.g. commercial enterprises, government agencies, not-for-profit organizations).

- ITU-T Recommendation X.1054 | ISO/IEC 27014: *Governance of information security*

  Publication date: 2013-05-15 – 11 pages

  ISO/IEC 27014:2013 provides guidance on concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security related activities within the organization. ISO/IEC 27014 is applicable to all types and sizes of organizations.

- ISO/IEC TR 27015: *Information security management guidelines for financial services*

  Publication date: 2012-12-01 – 18 pages

  ISO/IEC TR 27015:2012 provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

- ISO/IEC TR 27019: *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry*

  Publication date: 2013-07-15 – 37 pages

  ISO/IEC TR 27019:2013 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. The aim of ISO/IEC TR 27019 is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

  Note: ISO/IEC TR 27019 was prepared by DIN Deutsches Institut für Normung e. V. (as DIN SPEC 27009:2012-04) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, Information technology, in parallel with its approval by the national bodies of ISO and IEC. It has been assigned by the JTC 1 Secretariat to SC 27 programme of work.

- ISO/IEC 27033-5: *Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

  Publication date: 2013-07-31 – 14 pages

ISO/IEC 27033-5:2013 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.

- ISO/IEC 27037: *Guidelines for identification, collection, acquisition and preservation of digital evidence*

  Publication date: 2012-10-15 – 38 pages

  ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

- ISO/IEC 29115: *Entity authentication assurance framework*

  Publication date: 2013-04-01 – 36 pages

  ISO/IEC 29115:2013 provides a framework for managing entity authentication assurance in a given context. In particular, it specifies four levels of entity authentication assurance, and criteria and guidelines for achieving each of the four levels of entity authentication assurance. It further provides guidance for mapping other authentication assurance schemes to the four levels, guidance for exchanging the results of authentication based on the four levels, and guidance concerning controls that should be used to mitigate authentication threats.

- ISO/IEC 29191: *Requirements for partially anonymous, partially unlinkable authentication*

  Publication date: 2012-12-15 – 9 pages

  In many types of transactions, entities prefer to remain anonymous and unlinkable, which means that when two transactions are performed, it is difficult to distinguish whether the transactions are performed by the same user. However, in some circumstances there are legitimate reasons to enable subsequent reidentification by an a priori designated opener. ISO/IEC 29191:2012 provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.

- ISO/IEC 29192-4 *Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques*

  Publication date: 2013-06-01 – 26 pages

  ISO/IEC 29192-4:2013 specifies three lightweight mechanisms using asymmetric techniques, a unilateral authentication mechanism based on discrete logarithms on elliptic curve, an authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key, and an identity-based signature mechanism.

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

2.2.2 Documents awaiting Publication

The following International Standards or Technical Reports developed by SC 27 have been finalized and are awaiting publication:

- ISO/IEC 15408-1: *Evaluation criteria for IT security -- Part 1: Introduction and general model* (to be published as corrected and reprinted version of 3rd ed. 2009-12-15)
- ISO/IEC 18045: *Methodology for IT security evaluation* (to be published as corrected and reprinted version of 2nd ed. 2008-08-15)
- ISO/IEC 20008-1: *Anonymous digital signatures -- Part 1: General*
- ISO/IEC 20008-2: *Anonymous digital signatures -- Part 2: Mechanisms using a group public key*
- ISO/IEC FDIS 27001: *Information security management systems -- Requirements* (2nd ed.)
- ISO/IEC FDIS 27002: *Code of practice for information security controls* (2nd ed.)
- ISO/IEC DTR 27016: *Information security management -- Organizational economics*
- ISO/IEC FDIS 27033-4: *Network security -- Part 4: Securing communications between networks using security gateways* (revision of 1st edition of 18028-3:2005)
- ISO/IEC 27036-1: *Information security for supplier relationships -- Part 1: Overview and concepts*
- ISO/IEC 27036-2: *Information security for supplier relationships -- Part 2: Requirements*
- ISO/IEC 27036-3: *Information security for supplier relationships -- Part 3: Guidelines for ICT supply chain security*
- ISO/IEC DIS 27039: *Selection, deployment and operations of intrusion detection and prevention systems (IDPS)* (revision of 18043, 1st ed. 2006-06-15)
- ISO/IEC FDIS 29101: *Privacy architecture framework*
- ISO/IEC FDIS 29147: *Vulnerability disclosure*
- ISO/IEC 30111: *Vulnerability handling processes*

2.3 Resources

The last SC 27 Plenary meeting took place April 29–30, 2013 in Sophia Antipolis, France and was attended by 65 delegates from 27 of the current 51 P-members.

The five SC 27 Working Groups held meetings April 22–26, 2013 in Sophia Antipolis, France and October 22–26, 2012 in Rome, Italy. In average, these WG meetings were attended by more than 280 delegates in total with many delegates attending several Working Groups.

The next Working Group meetings are scheduled for October 21–25, 2013 in Incheon, Republic of Korea. The next SC 27 Plenary will take place April 14–15, 2014 in Hong Kong, China and will be preceded by meetings of the five Working Group, April 7–11, 2014 at the same location.

Overall, the resources and expertise prove to be sufficient to meet the many challenges SC 27 is facing. For selected projects, SC 27 resources are complemented by resources from appropriate SC 27 liaison organizations.

The 6-month meeting cycle of SC 27 is a good end efficient tradition, as it allows holding meetings at about the same time every year and does not charge too much on delegates' budgets.

In order to further improve the efficiency of SC 27 and its WGs, to increase the quality of deliverables, to define the right balance between WG autonomy and coordination at SC 27 level, and to make optimal use of the relevant ISO processes and tools available, SC 27 resolved to establish two Special Working Groups, one on Management (SWG-M) and one on Transversal Items (SWG-T).

3 Focus Next Work Period

3.1 Deliverables

Deliverables expected from the next work period (October 2013 - September 2014) include

- ISO/IEC 11770-3: *Key management -- Part 3: Mechanisms using asymmetric techniques* (3rd ed)
- ISO/IEC 18014-4: *Time-stamping services - Part 4: Traceability of time sources*
- ISO/IEC 18033-1: *Encryption algorithms -- Part 1: General* (2nd ed.)
- ISO/IEC 18033-5: *Encryption algorithms – Part 5: Identity-based ciphers*
- ISO/IEC 20009-2: *Anonymous entity authentication -- Part 2: Mechanisms based on signatures using a group public key*
- ISO/IEC TR 27016: *Information security management -- Organizational economics*
- ISO/IEC 24760-2: *A framework for identity management -- Part 2: Reference architecture and requirements*
- ISO/IEC 27018: *Code of practice for PII protection in public clouds acting as PII processors*
- ISO/IEC 27033-4: *Network security -- Part 4: Securing communications between networks using security gateways* (revision of 1st edition of 18028-3:2005)
- ISO/IEC 27036-1: *Information security for supplier relationships -- Part 1: Overview and concepts*
- ISO/IEC 27036-2: *Information security for supplier relationships -- Part 2: Requirements*
- ISO/IEC 27036-3: *Information security for supplier relationships -- Part 3: Guidelines for ICT supply chain security*
- ISO/IEC 27038: *Specification for digital redaction*
- ISO/IEC 27039: *Selection, deployment and operations of intrusion detection and prevention systems (IDPS)* (revision of 18043:2006)
- ISO/IEC 29146: *A framework for access management*
- ISO/IEC 29147: *Vulnerability disclosure*
- ISO/IEC 29190: *Privacy capability assessment model*

- ISO/IEC TS 30104: *Physical security attacks , mitigation techniques and security requirements*

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 detailed, sector-specific guidance for selected 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, TC 68/SC 2 and ITU-T.

3.2.1 Challenges

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

For some specific standards, such as cryptographic algorithms, cryptographic parameter generation, etc., internal SC 27 resources are not sufficient to conduct appropriate security evaluation and to ensure the desired quality. In these cases, SC 27 needs to ensure to establish the necessary cooperation with external initiatives in this area.

3.2.2 Opportunities

Standardized security techniques are becoming mandatory requirements for e- and m-commerce, e-government, health-care, and many other application areas. The use of security techniques and in particular of identification, authentication and 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 sector.

Growing awareness, concerns and opportunities with regard to privacy in society offer another area of opportunity for SC 27.

3.2.3 Marketing Initiatives and Joint Standardization Events

SC 27 has established the position of a PR officer, whose role is to produce and distribute a number of press releases and articles each year. These aim at promoting the standards that SC 27 develops and publishes. The press releases are targeted at users, auditors, implementers and management in all sectors of industry and commerce. The distribution channels include international user groups and associations interested in security standards, security journals, ISO 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).

SC 27 has continued to promote its standards work to the wider user community through articles and press releases in conjunction with the ISO publishing house. Experts working in all SC 27 have been contributing papers, presentations and talks in many conferences, seminars and workshops at events around the world.

SC 27/SD11 provides a very accessible overview of the work of SC 27. This includes a number of the SC 27 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 SC 27 Web site http://www.jtc1sc27.din.de/en

On the occasion of its 20th birthday, the "SC 27 Platinum Book – Twenty Years of ISO/IEC JTC 1/SC 27 Information Security Standardization" has been produced. Included in this book are many articles written by experts working in SC 27 as well as by current and past officers of SC 27. The book further contains statements by SC 27 liaison organizations as well as by some National Bodies. An electronic version is available from the SC 27 Web Site.

In July of this year SC 27 contributed to the planned JTC 1 'glossy' publication. The title of the SC 27 article for this JTC 1 publication is "SC 27 - International Centre of Expertise on Information Security". Also this year sees the publication of the second edition of the ISMS standards ISO/IEC 27001 and ISO/IEC 27002 – to promote these new editions a set of FAQ has been published on the ISO web site and an article on the use of ISO/IEC 27001 is being published by ISO in November this year. This article includes statements from senior management of companies in Australia, Brazil, China, Thailand and UK, as well as statistics relating to the current risk environment that business needs to operation in. The use of ISO/IEC 27001 helps business manage the risks that businesses face.

At its meeting in Incheon, Republic of Korea in October 2013, SC27 and Korean Industry are having a half-day seminar entitled 'Security in Cyberworld' which will explore the role of SC 27 standards to tackle cyber risks.

Over the years officers of SC 27 have been invited to take part and give presentations at many seminars and conferences including the joint Chinese/US symposium on Cyber-Security in October 2011 and the Cyber Security conference in Bangkok in March 2013.

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

3.3 Work Programme Priorities

Priority tasks for Working Group 1 include keeping the WG 1 Roadmap up-to-date, and to ensure effective and timely progression of:

- Revisions of ISO/IEC 27000 *Information security management systems - Overview and vocabulary*, ISO/IEC 27001 *Information security management systems - Requirements*, ISO/IEC 27002 *Code of practice for information security management*, ISO/IEC 27004 *Information security management measurements*, ISO/IEC 27006 *International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems* (in alignment with the systematic revision of ISOIEC 17021).
- Development of ISO/IEC TR 27016 *Information security management - Organizational economics* and ISO/IEC 27017 *Cloud computing security and privacy -- Security controls*
- Recently started work looking at Smart Grid Security and the Certification of Security Personal (in keeping with accreditation standard ISO 17024).

Also WG1 is starting work on the revision of ISO/IEC 27003 and ISO/IEC 27005 to align with the new edition of ISO/IEC 27001. In addition, WG 1's role in the cooperation with ITU-T is of strategic importance with regard to the ISO/IEC 27000

ISMS family of standards, and more recently in regard to the soon to be published ITU-T and SC27 joint standard on information security governance.

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 timely development of specifications for the recently established projects

- ISO/IEC 11770-6: *Key management – Part 6: Key derivation*
- ISO/IEC 20009-4: *Anonymous entity authentication – Part 4: Mechanisms based on weak secrets*
- ISO/IEC 29192-5: *Lightweight cryptography – Part 5: Hash-functions*

WG 2 has also started preparing the inclusion of SHA-3 into ISO/IEC 10118-3: *Hash-functions – Part 3: Dedicated hash-functions* under the WG 2 Study Period on Revision of ISO/IEC 10118-3.

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. All new IT security challenges, like cloud computing, or cyber security at large, demand secure technology, products, systems and services, and their security evaluation and testing is increasingly important, a demand that the WG 3 needs to address and provide responses to. The maintenance of the current WG 3 project catalogue is being challenged with new study periods and work item proposals that aim to address these new areas of IT security evaluation and testing.

In addition, there are several technical issues and domains of discussion where the WG 3 standards are well positioned to provide an international solution, like those related to cryptographic module security testing, and cryptography implementation conformance testing. Other technical areas and problems that will be worth exploring are those related to the security problems of supply chain and product specific protection profiles.

The projects in WG 4 can currently be divided into two main domains:

- Security incidents
  - Detection
  - Investigation
  - Management
  - Recovery

- System and system life cycle security
  - Acquisition and supply
  - Security related to storage
  - Security related to processing
  - Security related to communication

It is important that WG 4 focusses on addressing these topics within its scope of security controls and services. Because of the industry demand for International Standards in these areas (often with reference to cloud and cybersecurity), it is a priority to ensure that the correct documents are developed, and published without unnecessary delay. This is only possible through relevant and timely contributions from editors, members and by collaboration with relevant liaisons. It is also a priority to

ensure that the resulting International Standards and Technical Reports complement each other and that there is no unnecessary overlap.

Priorities for Working Group 5 are to complete foundational frameworks and architectures (e.g. project ISO/IEC 24760 *A framework for identity management*) 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 ISO/IEC 29146 *A framework for access management,* and ISO/IEC 29190 *Privacy capability assessment model.* Additionally, Working Group 5 has started new projects in the area of Telebiometric authentication (ITU-T X.1085 (bhsm) | ISO/IEC 17922), Cloud Computing (ISO/IEC 27018), Privacy Impact Assessment (ISO/IEC 29134), and Identity Proofing (ISO/IEC 29003). Moreover, there are Study Periods on Privacy Impact Assessment, Privacy / Personal Information Management Systems, security evaluation of anti-spoofing techniques for biometrics, Privacy Seal programs, and the documentation of data deletion principles for personally identifiable information in organisations. These projects and initiatives are also addressing recommendations from the ISO/TMB Privacy Steering Committee.