ISO/IEC JTC 1/SC 27 N15445

REPLACES: N14360

ISO/IEC JTC 1/SC 27

Information technology -- Security techniques

Secretariat: DIN, Germany

DOC TYPE: Business Plan

TITLE: SC 27 Business Plan October 2015 – September 2016

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2015-09-09

PROJECT:

STATUS: for submission to JTC 1

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
H. Cuschieri, B. Garcia, 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
A. Fuchsberger, F. Kahn, SWG-Convenors

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

NO. OF PAGES: 1 + 11

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.din.de/go/jtc1sc27

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

Period covered: October 2015 – September 2016

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 35 of the 27th SC 27 Plenary meeting in Kuching, Malaysia, 11th – 12th May 2015.

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 , security processes, and 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 management systems;
- 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: 230
- number of active projects: 83
- number of publications: 147

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, available at http://www.din.de/go/jtc1sc27.

1.3.2 New Projects and Study Periods

The following new projects have been approved over the past 12 months either via a 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 20543, *Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408;*
- ISO/IEC NP TR 20540, *Guidelines for testing cryptographic modules in their operational environment;*
- ISO/IEC NP 19086-4, *Cloud computing – Service Level Agreement (SLA) framework – Part 4: Security and privacy* (joint project between SC 27 and SC 38);
- ISO/IEC NP 20889, *Privacy enhancing data de-identification techniques.*

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

- ISO/IEC 11770-4, *Key management – Part 4: Mechanisms based on weak secrets* (revision of 1st ed. 2006-12-01);
- ISO/IEC 15946-5, *Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation* (revision of 1st ed. 2009-05-15);
- ISO/IEC 24761, *Authentication context for biometrics* (revision of 1st ed. 2009-05-15);
- ISO/IEC 27000, *Information security management systems — Overview and vocabulary* (revision of 3rd ed. 2014-01-15);
- ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications* (revision of 1st ed. 2014-04-01);
- ISO/IEC TR 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry* (revision of 1st ed. 2013-07-15);
- ISO/IEC 30111, *Vulnerability handling processes* (revision of 1st ed. 2013-11-01).

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

- Cloud security use cases and potential standardization gaps (WG 1);
- Information security code of practice for the aviation industry (WG 1);
- Review of definition processes and governance (WG 1);
- Cloud and new data technologies risk management (WG 1 and WG 4);
- Review of UK proposal for a new mechanism in ISO/IEC 11770-3 (WG 2);
- Amendment to ISO/IEC 29192-2 (WG 2);

- Lightweight MACs (WG 2);
- Inclusion of Chinese SM2 and IBS schemes in ISO/IEC 14888-3 (WG 2);
- Quantum computing resistant cryptography (WG 2);
- Inclusion of SM3 in ISO/IEC 10118-3 (WG 2);
- Inclusion of FACE in ISO/IEC 18033-2 (WG 2);
- Security information and event management (SIEM) realignment with current developments and processes (Future of SIEM) (WG 4);
- Virtualization security (WG 4);
- Study period on A privacy enhancing identity management scheme using attribute-based credentials (WG 5 together with WG 2);
- User friendly online privacy notice and consent (WG 5);
- On the adoption and usage of ISO/IEC 29115 and its interaction with ISO/IEC 29003 (WG 5);
- Privacy engineering framework (WG 5);
- Anonymous attribute assurance (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 7, WG 10, SC 6, SC 7, SC 17, SC 22, SC 25, SC 31, SC 36, SC 37, SC 38 and SC 40;
- within ISO including TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, TC 272, TC 292, ISO/CASCO, TMB/JTCG MSS, TMB/SAG;
- within IEC including IEC/ACSEC, IEC/SC 45A, IEC/TC 57, IEC/TC 65; and
- to external organizations including ABC4Trust, Article 29 Data Protection Working Party, CCDB, CDFS, CEN/TC 377, CSA, ENISA, EPC, ETSI, EuroCloud, FIDIS, FIRST, ICDPPC, INLAC, INTERPOL, ISACA, $(ISC)^2$, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, OpenID Foundation, PICOS, PRACTICE and VISA.

Currently SC 27 maintains 30 internal and 41 external liaisons. A complete list is available at www.din.de/go/jtc1sc27 / 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. In that respect, SC 27 contributed to the TC68/SC 2 overview document on Financial Services Security Framework and regularly provides liaison statements on specific topics such as ISMS and cryptographic algorithms.

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 15816:2002-02-01 (1st ed.), *Security information objects for access control;*
- Recommendation ITU-T X.842 | ISO/IEC TR 14516: 2002-06-15 (1st ed.), *Guidelines on the use and management of Trusted Third Party services* (currently under revision as a multi-part Technical Report consisting of three parts);
- Recommendation ITU-T X.843 | ISO/IEC 15945: 2002-02-01 (1st ed.), *Specification of TTP services to support the application of digital signatures;*
- Recommendation ITU-T X.1051 | ISO/IEC 27011: 2008-12-15 (1st ed.), *Information security management guidelines for telecommunications;*
- Recommendation ITU-T X.1054 | ISO/IEC 27014: 2013-05-15 (1st ed.), *Governance of information security;*
- Draft Recommendation ITU-T X.1085 (bhsm) | ISO/IEC CD 17922, *Telebiometric authentication framework using biometric hardware security module;*
- Draft Recommendation ITU-T X.1631 (cc-control) | ISO/IEC FDIS 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services;*
- Draft Recommendation ITU-T X.gpim | ISO/IEC CD 29151, *Code of practice for the protection of personally identifiable information.*

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 ISO TC 292 Security and resilience

ISO TC 292 was created as the result of an initiative to restructure the security sector within ISO. Its broad scope covers *Standardization in the field of security to enhance the safety and resilience of society.*. To avoid potential overlap and to ensure maximum effectiveness, SC 27 has established close cooperation with TC 292.

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, information and IT security has been at the forefront of information and communications technology (ICT). Both security and privacy have emerged high on the management agenda, have been the subject of new legislation and have made their way into many news headlines. For example, organizations deploying (remote) electronic services (e.g., e-business, e-government) need to ensure control over who has access to information and applications and what users are allowed to do once they have access. 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 IT 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 management), ISO 14001 (Environment management), ISO 22000 (Food safety management) and ISO 22301 (Business continuity management).

In addition, users ask more and more about protection of the privacy of their information and data. There is a close relationship between information and IT security and privacy. The issues being addressed are sometimes complex, and sensitive. 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 Working Group 5 "Identity Management and Privacy Technologies", e.g. by ISO/IEC 24760 "A rramework for identity management" and ISO/IEC 29100 "Privacy framework".

Standardized security techniques are becoming mandatory requirements for e- and m-commerce, health-care, telecoms, energy sector, automotive and many other application areas in both the commercial and government sectors. SC 27 is a centre of expertise for the standardization of security techniques for addressing the security and privacy requirements and market needs across many market sectors.

The short term future sees many market opportunities for SC 27 to expand the deployment of its standards and its expertise as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security, privacy, and IT security has been at the forefront of the related standardization for more than twenty-five years. It has the right mix of skills and resources to deliver security standards to market requirements as demonstrated 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. Furthermore, the "Internet of things", "Big Data" and other emerging technologies are gaining more and more attention. SC 27 has a study period addressing future standards defining how to manage the potential risks with regard to these new technologies. In addition, 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.

More and more, organizations are recognizing the importance of addressing security and privacy 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 2014, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:

- ISO/IEC 10118-4:1998/Amd.1:2014-11-15, *Hash-functions -- Part 4: Hash-functions using modular arithmetic -- Amendment 1: Object identifiers;*
- ISO/IEC 11770-3:2015-08-01 (3rd ed.), *Key management – Part 3: Mechanisms using asymmetric techniques;*
- ISO/IEC 18014-4:2015-04-15 (1st ed.), *Time-stamping services -- Part 4: Traceability of time sources;*
- ISO/IEC 18033-1:2015-08-01 *(2nd ed.) Encryption algorithms — Part 1: General;*
- ISO/IEC 24760-2:2015-06-01 *(1st ed.) A framework for identity management — Part 2: Reference architecture and requirements;*
- ISO/IEC TR 27023:2015-07-01 (1st ed.), *Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002;*
- ISO/IEC 27033-1:2015-08-15 (2nd ed.), *Network security - Part 1: Overview and concepts;*
- ISO/IEC 27034-2:2015-08-15, (1st ed.), *Application security -- Part 2: Organization normative framework;*
- ISO/IEC 27039:2015-01-15 (1st ed.), *Selection, deployment and operation of intrusion detection and prevention systems (IDPS);*
- ISO/IEC 27040:2015-01-15, (1st ed.), *Storage security;*
- ISO/IEC 27041:2015-06-15, (1st ed.), *Guidance on assuring suitability and adequacy of incident investigation methods;*
- ISO/IEC 27042:2015-06-15 (1st ed.), *Guidelines for analysis and interpretation of digital evidence;*
- ISO/IEC 27043:2015-03-01 (1st ed.), *Incident investigation principles and processes;*
- ISO/IEC 29190:2015-08-15 (1st ed.) *Privacy capability assessment model;*
- ISO/IEC TS 30104:2015-05-15 (1st ed.) *Physical security attacks, mitigation techniques and security requirements;*
- ISO/IEC 30121:2015-04-01 (1st ed,) *Information technology – Governance of digital forensic risk framework* (in collaboration with SC 40).

In addition, a number of 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 17825 (3rd or 4th Q. 2015) (1st ed.), *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*
- ISO/IEC 18033-5 (3rd or 4th Q. 2015) (1st ed.), *Encryption algorithms – Part 5: Identity-based ciphers*
- ISO/IEC TR 20004 (3rd or 4th Q. 2015) (2nd ed.), *Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*
- ISO/IEC 27010 (3rd or 4th Q. 2015) (2nd ed.), *Information security management for inter-sector and inter-organizational communications*
- ISO/IEC 29192-4:2013/Amd.1 (3rd or 4th Q. 2015), *Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques -- Amendment 1*

2.3 Resources

The last SC 27 Plenary meeting took place May 11-12, 2015 in Kuching, Malaysia and was attended by 61 delegates from 26 of the current 51 P-members.

The five SC 27 Working Groups held meetings May 4-8 May, 2015 in Kuching, Malaysia and October 2014 in Mexico City, Mexico. In both the Kuching and Mexico City meetings around 280 delegates spread across the five SC 27 Working Groups.

The next set Working Group meetings are scheduled for October 26-30, 2015 in Jaipur, India. The next SC 27 Plenary will take place April 18-19, 2016 in Tampa, FL, United States and will be preceded by meetings of the five SC 27 Working Groups, April 11-15, 2016 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 has proven to be an efficient use of resources for the development of standards. This 6-month cycle tradition allows holding meetings at about the same time every year and helps to minimize the delegates' travel 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 2015 - September 2016) include

- ISO/IEC 10116 (4th ed.), *Modes of operation for an n-bit block cipher*
- ISO/IEC 14888-3 (3rd ed.), *Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*
- ISO/IEC 11770-6 (2nd ed.), *Key management – Part 6: Key derivation*
- ISO/IEC 15946-1 (3rd ed.), *Cryptographic techniques based on elliptic curves – Part 1: General*
- ISO/IEC 18031:2011/Amd.1), *Random bit generation – Amendment 1*
- ISO/IEC 18367 (1st ed.), *Cryptographic algorithms and security mechanisms conformance testing*
- ISO/IEC 18370-1 (1st ed.), *Blind digital signatures – Part 1: General*
- ISO/IEC 18370-2 (1st ed.), *Blind digital signatures – Part 2: Discrete logarithm based mechanisms*

- ISO/IEC 24760-3 (1st ed.), *A framework for identity management -- Part 3: Practice*
- ISO/IEC 27000 (3rd ed.), *Information security management systems — Overview and vocabulary*
- ISO/IEC 27006 (3rd ed.), *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27009 (1st ed.) *Sector specific application of ISO/IEC 27001 – Requirements*
- ITU-T X.1051 | ISO/IEC 27011 (2nd ed.) *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*
- ISO/IEC 27013 (2nd ed.), *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
- ITU-T X.1631 (cc-control) | ISO/IEC 27017 (1st ed.), *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27033-6 (1st ed.), *Network security -- Part 6: Securing wireless IP network access*
- ISO/IEC 27034-6 (1st ed.), *Application security -- Part 6: Case studies*
- ISO/IEC 27035-1 (1st ed.), *Information security incident management -- Part 1: Principles of incident management*
- ISO/IEC 27035-2 (1st ed.), *Information security incident management -- Part 2: Guidelines to plan and prepare for incident response*
- ISO/IEC 29146 (1st ed.), *A framework for access management*
- ISO/IEC 29192-5 (1st ed.), *Lightweight cryptography – Part 5: Hash-functions*

3.2 Strategies

SC 27's core 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 information and IT security is the cooperation with such users, such as SC 7, SC 17, SC 25, SC 36, SC 37, SC 38, SC 40, JTC 1/WG 7, JTC 1/WG 10, TC 68/SC 2, TC 292, and ITU-T, and all the other organisations under clause 1.4 that SC cooperates with..

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 and suitability 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 technical 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 Communications Officer, whose role is to promote the work of SC 27 through different channels: press releases and articles, conferences and workshops, interactive ISO chat forums and other media channels, as well as though Wikipedia. This effort is aimed at promoting the broad and detailed scope of 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, and for government users. 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 management and experts working contribute to papers, presentations and talks in many conferences, seminars and workshops at events around the world.

The SC 27 publication standing document SD11 provides a very accessible overview of the work of SC 27.SD11 is freely available to everyone and is downloadable via the SC 27 Web site http://www.din.de/go/jtc1sc27.

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 Spring 2015 SC27 celebrated its 25th birthdaywith a further 'birthday book", which was launched at its Plenary and WG meetings in Kuching, Sarawak, Malaysia .

At most of its WG meetings SC 27 engages with local industry to hold a knowledge transfer workshops. At the SC 27 meeting in Hong Kong (April 2014), SC 27 collaborated with the department of the Hong Kong responsible for IT Services to run a very successful workshop on SC 27 standards and the implementation of these standards by businesses in Hong Kong. Workshops were held at the last two WG meetings in Mexico City and Kuching, Sarawak, and a further workshop is planned for the next SC 27 meetings in Jaipur, India (October 2015).

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 conferences in Bangkok in March 2013 and July 2014. In September 2014 the Chair of SC 27 and the Convenor of WG 1 took part in the ITU-T SG17 workshop on security standardization for developing countries.

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

3.3 Work Programme Priorities

3.3.1 Working Group 1

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

Projects under revision;

- ISO/IEC 27000 *Overview and vocabulary (revision of 3rd ed.);*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems* (revision of 2nd ed.) (in alignment with the systematic revision of ISOIEC 17021);
- ISO/IEC 27007 *Guidelines for information security management systems auditing (revision of 3rd ed.);*
- ISO/IEC TR 27008 *Guidelines for auditors on ISMS controls (revision of 3rd ed.);*

- ISO/IEC 27010 *Information security management for inter-sector and inter-organisational communications (revision of 3rd ed.);*
- Recommendation ITU-T X.1051 | ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002* (revision of 1st ed.) ISO/IEC 27013, *Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC* 20000-1 (revision of 1st ed.)
- ISO/IEC 27003, 27004 and 27005 the suite of guidelines supporting the new edition of ISO/IEC 27001:2013 (revisions of 1st ed.)
- ISO/IEC TR 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (revision of 1st ed.).*

Projects under development

- ISO/IEC 27009, *Sector-specific application of ISO/IEC 27001 – Requirements;*
- ITU-T X.1631 | ISO/IEC 27017, (Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002);
- *Recommendation* ITU-T X.1631 (cc-security) | ISO/IEC 27017, *Code of practice fo information security controls based on ISO/IEC 27002 for cloud services;*
- ISO/IEC 27021 R*equirements for information security management professionals.*

3.3.2 Working Group 2

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 19592-1 (1st ed.), *Secret sharing – Part 1: General*
- ISO/IEC 19592-2 (1st ed.), *Secret sharing – Part 2: Fundamental mechanisms*
- ISO/IEC 20009-4: *Anonymous entity authentication – Part 4: Mechanisms based on weak secrets*

In addition, WG 2's roles in the cooperation with TC 68 Banking and Related Financial Services are of strategic importance.

3.3.3 Working Group 3

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. As indicated in the WG 3 road map, there is a need to define a security conformity testing framework compatible and complementing ISO/IEC 15408 for lower assurance levels of security evaluation. A number of device specific evaluation and testing security requirements may be demanded from the market in the short term.

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.

3.3.4 Working Group 4

Work is continuing on projects in the area of

- eDiscovery (ISO/IEC 27050, currently in working draft);
- Guidelines for the use and management of electronic trust service providers (ISO/IEC TR 14516, currently in working draft);
- Application security (ISO/IEC 27034);
- Network security (ISO/IEC 27033); and
- Cloud computing (ISO/IEC 19086-4 and various study periods)

A priority is the publication of

- ISO/IEC 27035-1, *Information security incident management – Part 1: Principles of incident management;*
- ISO/IEC 27035-2, *Information security incident management – Part 2: Guidelines to plan and prepare for incident response;* and
- ISO/IEC 27034-6, *Application security – Part 6: Security guidance for specific applications.*

3.3.5 Working Group 5

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. An example is ISO/IEC 29146 *A framework for access management.* More recent projects are in the area of telebiometric authentication (ITU-T X.1085 (bhsm) | ISO/IEC 17922), *Privacy impact assessment* (ISO/IEC 29134), *Identity proofing* (ISO/IEC 29003), and *Code of practice for personally identifiable information protection* (ISO/IEC 29151). Moreover, there are Study Periods on *A privacy enhancing identity management scheme using attribute-based credentials* (together with WG 2) , *User friendly online privacy notice and consent, A Privacy Engineering Framework ,* and *Anonymous attribute assurance*.