ISO/IEC JTC 1/SC 27 N18950

REPLACES: N18780

ISO/IEC JTC 1/SC 27

Information technology -- Security techniques

Secretariat: DIN, Germany

DOC TYPE:	**Business Plan (defined)**
TITLE:	**SC 27 Business Plan and Dashboard, IT Security techniques**
SOURCE:	**Andreas Wolf, SC 27 Chairman (acting)**
DATE:	2018-09-25
PROJECT:	
STATUS:	**for submission to JTC 1**
ACTION ID:	**Info**
DUE DATE:	
DISTRIBUTION:	P, O, L Members L. Rajchel, JTC 1 Secretariat Ch.-P. Brazin de Caix, ITTF A. Wolf, Acting SC 27 Chairman M. De Soete, SC 27 Vice-Chair T. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors J.-P. Quémard, MAG Convenor A. Fuchsberger, SWG-T Convenor
MEDIUM:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27
NO. OF PAGES:	1 + 12 + 1 (Attachment 1)

ISO/IEC JTC 1/SC 27 N18950

BUSINESS PLAN FOR JTC 1/SC 27

Information technology – Security techniques

PERIOD COVERED: October 2018 – September 2019

1.0 Executive summary (limit achievements to those suitable for publicity)

SC 27 is an international recognized centre of expertise serving the needs of many business sectors as governments. Its work covers both management standards as well as technical standards. SC 27 has brought together many of the world's leading information security and privacy experts, which so far has led to more than 180 publications, among them one of the three most popular standards within ISO.

Committee membership has increased from 18 P-members in 1990 to 51 P-members (plus 25 O-members) in 2018, covering a vast area of the globe.

Focusing on the development of generic standards for the protection of information and ICT has led to a large number of liaisons to SDOs and industry bodies which typically use SC 27 standards as a basis for developing their own sector-specific security implementation standards.

2.0 Chairman's Remarks

This Business Plan has been prepared in accordance with Resolution 34 of the 30th SC 27 Plenary meeting in Wuhan, Hubei Province, China, 23-24 April 2018.

2.1 Market Requirements, Innovation

The current era of information revolution, rapid development of Internet and other information technologies brings along substantial changes in many areas – from our daily life to the means and methods of industrial production. With this transition, standardized security techniques are becoming mandatory requirements across almost any sector.

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 almost thirty 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.

2.2 Accomplishments

2.2.1 Publications

Since October 2017, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:

- ISO/IEC 11770-3:2015/Amd. 1:2017-11 — Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques — AMENDMENT 1: Blinded Diffie-Hellman key agreement
- ISO/IEC 11770-4:2017-11 (2nd edition) — Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets
- ISO/IEC 18033-2:2006/Amd. 1:2017-11 — Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers — AMENDMENT 1: FACE
- ISO/IEC 19592-2:2017-10 (1st edition) — Information technology — Security techniques — Secret sharing -- Part 2: Fundamental mechanisms
- ISO/IEC 19896-1:2018-01 (1st edition) — Competence requirements for information security testers and evaluators -- Part 1:
- ISO/IEC 19896-2:2018-08 (1st edition) — Competence requirements for information security testers and evaluators -- Part 2:
- ISO/IEC 19896-3:2018-08 (1st edition) — Competence requirements for information security testers and evaluators -- Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
- ISO/IEC 20008-2:2013-11 (1st edition) (corrected 2017-11) — Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key
- ISO/IEC TS 20540:2018-05 (1st edition) — Information technology — Security techniques — Testing cryptographic modules in their operational environment
- ISO/IEC 27000:2018-02 (5th edition) — Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27005:2018-07 (3rd edition) — Information security risk management
- ISO/IEC 27019:2017-10 (2nd edition) — Information technology — Security techniques — Information security controls for the energy utility industry
- ISO/IEC 27021:2017-10 (1st edition) — Information technology — Security techniques — Competence requirements for information security management systems professionals
- ISO/IEC 27034-3:2018-05 (1st edition) — Information technology — Application security — Part 3: Application security management process
- ISO/IEC TS 27034-5-1:2018-04 (1st edition) — Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas
- ISO/IEC 27034-7:2018-05 (1st edition) — Information technology — Application security — Part 7: Assurance prediction framework

- ISO/IEC 27050-3:2017-10 (1st edition) — Information technology — Security techniques — Electronic discovery — Part 3: Code of practice for electronic discovery
- ISO/IEC TR 27103:2018-02 (1st edition) — Information technology — Security techniques
- ISO/IEC TS 29003:2018-03 (1st edition) — Information technology — Security techniques — Security techniques — Identity proofing

2.3 Resources

The last SC 27 Plenary meeting took place April 23 – 24 2018 in Wuhan, Hubei Province, China and was attended by 81 delegates from 31 of the current 51 P-members.

The five SC 27 Working Groups held meetings April 16 – 20 2018 in Wuhan, Hubei Province, China, and October 30 – 3 November 2017 in Berlin, Germany. In both the Wuhan and Berlin meetings around 280 delegates attended the five SC 27 Working Groups.

The next set of Working Group meetings are scheduled for September 30 – October 4 2018 in Gjøvik, Norway,. The next SC 27 Plenary will take place April 8 – 9 2019 in Tele-Aviv, Israel and will be preceded by meetings of the five SC 27 Working Groups, April 1 – 5 2019 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 current 6-month meeting cycle of SC 27 has shown 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 the style of management system type continual improvement regarding the efficiency and quality of work and deliverables within SC 27 and its WGs; achieving 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 has established an SC 27 Advisory Group and a Special Working Group on Transversal Items (SWG-T).

2.4 Competition and Cooperation (including consortia)

SC 27 benefits from collaboration with an extremely large number of productive and valuable liaisons with many organizations

- within ISO/IEC JTC 1 including WG 7, WG 11, SC 6, SC 7, SC 17, SC 22, SC 25, SC 31, SC 36, SC 37, SC 38, SC 40, SC 41 and SC 42;
- within ISO including TC 22, TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, ISO/TC 171, TC 272, TC 292, ISO/PC 302, ISO/TC 307, ISO/TC 309, ISO/CASCO, TMB/JTCG MSS, TMB/SAG;
- within IEC including IEC/ACSEC, IEC/SC 45A, IEC/TC 57, IEC/TC 65; IEC SC 121A and
- to external organizations including ABC4Trust, European Data Protection Board , CallConnect, CCDB, CEN/CENELEC JTC 8, CEN/CENELEC JTC 13, CEN/TC 377, CEN/TC 428, CREDENTIAL, CSA, ENISA, EPC, ETSI, FIRST, Global Platform, ICDPPC, IEEE, IFAA, INLAC, INTERPOL, ISACA, (ISC)^2, ISA99, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, OASIS, OECD, OpenID Foundation, PICOS, PQCRYPTO, PRIPARE, SAFEcrypto, Small Business Standards, TM Forum and WITDOM.

Currently SC 27 maintains 48 internal and 52 external liaisons. A complete list is available at www.din.de/go/jtc1sc27 / "Members".

Selected aspects related to these liaisons are highlighted below.

2.4.1 SC 37 'Biometrics'

There is a close and advantageous synergy exists between biometrics and IT security. The potential contribution of SC 27 to biometrics standards is evident. Particularly, in 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'.

2.4.2 ITU-T Q3/SG 17 and ITU-T FG Cloud Computing

ITU-T Q3/SG17 and SC 27 collaborate on several projects to progress common or twin text documents and to publish common standards. These projects include

- Recommendation ITU-T X.841 │ ISO/IEC 15816: 2002-02 (1st ed.), "Security information objects for access control";
- Recommendation ITU-T X.842 │ ISO/IEC TR 14516: 2002-06 (1st ed.), "Guidelines on the use and management of Trusted Third Party services";
- Recommendation ITU-T X.843 │ ISO/IEC 15945: 2002-02 (1st ed.), "Specification of TTP services to support the application of digital signatures";
- Recommendation ITU -T X.1051 │ ISO/IEC 27011: 2008-12 (1st ed.), "Information security management guidelines for telecommunications";
- Recommendation ITU-T X.1054 │ ISO/IEC 27014: 2013-05 (1st ed.), "Governance of information security";
- Draft Recommendation ITU-T X.1085 (bhsm) │ISO/IEC 17922*, "Telebiometric authentication framework using biometric hardware security module";
- Recommendation ITU-T X.1631 (cc-control) | ISO/IEC 27017: 2015-12-15, "Code of practice for information security controls based on ISO/IEC 27002 for cloud services";
- Draft Recommendation ITU-T 1058 (X.gpim) │ISO/IEC 29151, "Code of practice for the protection of personally identifiable information".

2.4.3 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.

2.4.4 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.

2.4.5 ISO/TC 307 Blockchain and distributed ledger technologies

ISO/TC 307 scope was created in 2016 and had its inaugural meeting in April 2017. This new committee has its scope the "*Standardisation of blockchains technologies and distributed ledger technologies*" and intends to cover not only the technologies used to implement and support blockchain and distributed ledgers, but also develop generic work to taking requirements of their application in sector specific environments.

Many of the fundamental technologies used by blockchain and distributed ledgers have standards that have already been developed in SC 27. As such SC 27 has engaged in an active liaison relationship to support the new work of TC 307. A significant number of SC 27 experts are also active in TC 307.

3.0 Discussion of SC 27 programme of work –

3.1 WG 1 – Information security management systems

SC 27/WG 1 develops, manages and maintains the family of ISO/IEC 27001 ISMS standards: management system requirements, supporting codes of practice and implementation guidelines, information security governance, ISMS auditing and certification standards, ISMS sector-specific controls and ISMS applied to protection in cyberspace. The complete SC 27/WG1 programme of work can be found described in SC 27 Standing Document SD18. It is also available from SC 27 public website at www.din.de/go/jtc1sc27

3.1.1 WG 1 accomplishments (last year)

Over the last twelve months WG 1 has completed work on successful revised versions of the following International Standards:

- ISO/IEC 27000: 2018-02 (5th edition), Information security management systems - Overview and vocabulary,
- ISO/IEC 27005:2018-07 (3rd edition), Information security risk management
- ISO/IEC 27019:2017-10 (2nd edition), Information technology — Security techniques — Information security controls for the energy utility industry
- ISO/IEC 27021:2017-10 (1st edition), Information technology — Security techniques — Competence requirements for information security management systems professionals
- ISO/IEC 27003:2017-03 (2nd edition), Information security management systems implementation – Guidance
- ISO/IEC 27007:2017-10 (2nd edition), Guidelines for information security management systems auditing,
- ISO/IEC 27019:2017-10 (2nd edition), Information security controls for the energy utility industry.

WG1 also published the 1st edition of the following deliverables:

- ISO/IEC 27021:2017-10 (1st edition), Competence requirements for information security management systems professionals
- ISO/IEC TR 27103:2018-02 (1st edition), Cybersecurity and ISO and IEC standards.

WG 1 has progressed work on the revised version of ISO/IEC TR 27008 "Guidelines for auditors on ISMS controls" with its publication as Technical Specification expected by the end of 2018.

3.1.2 WG 1 deliverables (this year and future)

WG 1 is progressing the development of a number of cybersecurity specific standards including:

- ISO/IEC 27100 (approved NWIP) Cybersecurity – Overview and concepts
- ISO/IEC 27101 (WD) Cybersecurity Framework development guidelines
- ISO/IEC 27102 (CD) Guideline for cyber insurance.

Other deliverables include the Standing Documents SD 7 (Use of ISO/IEC family of standards in Governmental / Regulatory requirements), SD 2 (Guidance and terminology processes) and SD 8 (Use Case Examples for the Application of ISO/IEC 27009).

The coming year will see the revision of ITU-T X.1054 | ISO/IEC 27014 (Governance of information security) and ISO/IEC 27002 (Code of practice for information security controls), and a PDAM for ISO/IEC 27006.

Finally, WG 1 is expected to embark in the near future on work in the field on security for lottery and gambling systems, in particular, starting with the future revision and maintenance IWA7.

3.1.3 WG 1 strategies/risks/opportunities/lessons learned (if any)

The established market position of ISO/IEC 27001 and ISO/IEC 27002 as bestselling ISO/IEC standards in information security management and as a common international language provides many opportunities for growth and outreach into all market sectors, especially to address the diverse and continual increase in cyber risks. The work of WG 1 provides both horizontal and vertical sector standards to ensure the necessary and appropriate outreach for customer demands and requirements. Given the success of the ISO/IEC 27000 family of standards, WG 1 programme of work attracts the attention of other ISO and IEC TCs and JTC1 SCs – this presents many opportunities in the application of the ISO/IEC 27000 family of standards across many domains of standardisation.

WG 1 continues to play a pro-active role in ISO/JTCG Joint technical Coordination Group on MSS (TAG 13) in shaping the future structure of MSS. Also, WG 1 actively liaises with IAF and CASCO concerning several aspects of MSS auditing and certification, as well as with other committees dealing with MSS such as ISO/TC 292, ISO/PC 302 and ISO/TC 262, and with IEC committees TC 45, TC 57 and TC 65 on cyber and sector-specific aspects of the WG1 ISMS projects.

3.2 WG 2 – Cryptography and security mechanisms

WG 2 deals with cryptography and security mechanisms. The Terms of Reference of WG 2 are (1) identifying the need and requirements for these techniques and mechanisms in IT systems and applications and (2) developing terminology, general models and standards for these techniques and mechanisms for use in security services.

The scope covers both cryptographic and non-cryptographic techniques and mechanisms including confidentiality, entity authentication, non-repudiation, key management and data integrity such as message authentication, hash-functions and digital signatures.

3.2.1 WG 2 accomplishments

In 2017, nine standards have been published.

- ISO/IEC 10116, Modes of operation for an n-bit block cipher algorithm
- ISO/IEC 14888-3 (Corrected edition), Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms
- ISO/IEC 11770-3/ADM1, Key management – Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 11770-4, Key management – Part 4: Mechanisms based on weak secrets
- ISO/IEC 15946-5, Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation
- ISO/IEC 18033-2/AMD1, Encryption algorithms – Part 2: Asymmetric ciphers – Amendment 1
- ISO/IEC 20009-4, Anonymous entity authentication – Part 4: Mechanisms based on weak secrets
- ISO/IEC 20008-2 (Corrected edition), Anonymous digital signatures – Part 2: Mechanisms using a group public key
- ISO/IEC 19592-2, Secret sharing – Part 2: Fundamental mechanisms

3.2.2 WG 2 deliverables

The following standards will be published in 2018.

- ISO/IEC 9798-3, Entity authentication – Part 3: Mechanisms using digital signature techniques
- ISO/IEC 10118-3, Hash-functions – Part 3: Dedicated hash-functions
- ISO/IEC 11770-2, Key management – Part 2: Mechanisms using symmetric techniques

3.2.3 WG 2 strategies/risks/opportunities/lessons learned (if any)

WG 2 currently has a set of criteria for the inclusion of new algorithms/mechanisms in

ISO/IEC 18033 (Encryption algorithms) and ISO/IEC 29192 (Lightweight cryptography).

3.3 WG 3 – Security evaluation, testing and specification

WG 3 covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

a) security evaluation criteria;

b) methodology for application of the criteria;

c) security functional and assurance specification of IT systems, components and products;

d) testing methodology for determination of security functional and assurance conformance;

e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

3.3.1 WG 3 accomplishments

The following products were published during 2017/2018:

- ISO/IEC TR 15446:2017-10 (3rd edition), Guidance for the production of Protection Profiles and Security Targets
- ISO/IEC TS 19249:2017-10 (1st edition), Catalogue of architectural and design principles for secure products, systems, and applications
- ISO/IEC 19896-1:2018-02 (1st edition), Competence requirements for information security testers and evaluators -- Part 1:
- ISO/IEC 19896-2:2018-08 (1st edition), Competence requirements for information security testers and evaluators -- Part 2:
- ISO/IEC 19896-3:2018-08 (1st edition), Competence requirements for information security testers and evaluators -- Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
- ISO/IEC TS 20540:2018-05 (1st edition), Information technology — Security techniques — Testing cryptographic modules in their operational environment

3.3.2 WG 3 deliverables

The following products have been, or are to be published, during 2018/2019:

- ISO/IEC TS 19608 (1st edition), Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
- ISO/IEC 19989-1 (1st edition), Criteria and methodology for security evaluation of biometric systems - Part 1: Framework
- ISO/IEC 20085-1 (1st edition), Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques
- ISO/IEC 20543 (1st edition), Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

3.3.3 WG 3 strategies/risks/opportunities/lessons learned (if any)

WG 3 has initiated the revision of ISO/IEC 15408 and ISO/IEC 18045, which are the cornerstone of its catalogue of projects and competence. This revision has special relevance, in the sense that it is the first time that WG 3 leads the maintenance and evolution of the referred standards, always in close coordination with the CCDB. This revision is scheduled to be completed in 2020, aiming to provide an improved standard able to cope with the new demands of cybersecurity evaluation and certification.

3.4 WG 4 – Security controls and services

The scope of WG 4 covers aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems. The topics covered include:

1. ICT security operations (for example readiness, continuity, incident and event management, investigation)
2. Information lifecycle (for example creation, processing, storage, transmission and disposal)
3. Organizational processes (for example design, acquisition, development and supply)
4. Security aspects of Trusted services (for example in the provision, operation and management of these services)
5. Cloud, internet and cyber security related technologies and architectures (for example network, virtualization, storage)

for digital environments, such as:

- Cloud computing
- Cyber
- Internet
- Organizations

3.4.1 WG 4 accomplishments

The following products were published during 2017/2018:

- ISO/IEC 27050-3:2017-10 (1st edition), Information technology – Security techniques – Electronic discovery – Part 3: Code of Practice for electronic discovery
- ISO/IEC 27034-3:2018-05 (1st edition), Information technology – Application security – Part 3: Application security management process
- ISO/IEC 27034-5:2018710 (1st edition), Information technology – Application security – Part 3:
- ISO/IEC TS 27034-5-1:2018-04 (1st edition), Information technology – Application security – Part 5-1: Protocols and application security controls data structure, XML schemas
- ISO/IEC 27034-7:2018-07 (1st edition), Information technology – Application security – Part 7: Assurance prediction framework

3.4.2 WG 4 deliverables

The following products are expected to be published in 2018-10/2019-09:

- ISO/IEC 27050-2, Information technology – Electronic discovery – Part 2:

Guidance for governance and management of electronic discovery

- ISO/IEC 19086-4, Information technology – Cloud computing – Service Level Agreement (SLA) framework – Part 4: Components of security and of protection of PII
- ISO/IEC 21878, Information technology – Security techniques – Security guidelines for the design and implementation of virtualized servers

3.4.3 WG 4 strategies/risks/opportunities/lessons learned (if any)

The need for International Standards in cybersecurity, cloud computing and virtualisation is rapidly growing. As such, more and more projects are be proposed and started in WG 4 in these areas.

WG 4 also continues to work in collaboration with other committees on matters such as big data, cloud computing and cybersecurity.

3.5 WG 5 – Identity management and privacy technologies

After completion of foundational frameworks (especially ISO/IEC 24760 A framework for identity management and ISO/IEC 29100 Privacy framework) priorities for Working Group 5 are to develop related standards and Standing Documents on supporting technologies, models, and methodologies.

3.5.1 WG 5 accomplishments

The following products were published during 2017/2018

- ISO/IEC 29134:2017-06 (1st edition), Guidelines for privacy impact assessment (1st edition)
- ITU-T X.1085 (bhsm) | ISO/IEC 17922:2017-09 (1st edition), Telebiometric authentication framework using biometric hardware security module
- ISO/IEC TS 29003:2018-03 (1st edition) “Identity proofing”
- ITU-T X.1058 (gpim) | ISO/IEC 29151:2017-08 (1st edition), Code of practice for personally identifiable information protection"
- ISO/IEC 29100:2011/Amd.1:2018-06, Privacy framework – Amendment 1"
- WG 5 Standing Document 2 – Privacy references list
- WG 5 Standing Document 4 – Standards Privacy Assessment

3.5.2 WG 5 deliverables

The following products are expected to be published in 2018/2019

- ISO/IEC 24760-1:2011/Amd.1, A framework for identity management – Part 1: Terminology and concepts – Amendment 1
- ISO/IEC 24761 (2nd edition), Authentication context for biometrics
- ISO/IEC 20889, Privacy enhancing data de-identification techniques

3.5.3 WG 5 strategies/risks/opportunities/lessons learned (if any)

More and more innovative privacy and identity management legislation around the world relies more on standards than in the past, which is a challenge and an opportunity. WG 5 is maintaining many liaisons. Liaisons with research projects have turned out to be successful: Relevant content was contributed and more volunteers were kept also in the longer perspective.

The proposal “Privacy by design for consumer goods and services” (ISO/NP 23485) developed by ISO/COPOLCO could have well been placed in WG 5 and WG 5 was willing to pick it up. However the ISO TMB after some discussion decided to establish a new PC, ISO/PC 317. The major reason mentioned later was, that JTC 1 lacks a COPOLCO representation (which indeed should be established to ease consumer participation in relevant JTC 1 projects). Obviously an extra PC on rather general privacy topics leads to the danger of fragmentation of the volunteer base, whose (travel) resources are limited anyway. WG 5 attempts to overcome this risk by close collaboration with PC 317 and ideally joint or back-to-back meetings.

3.6 Management Advisory Group (MAG)

The SC 27 Management Advisory Group (MAG) is a new internal administrative created to review and evaluate the effectiveness of SC27 and make recommendations for improvement. It was created following the 2017 SC 27 Heads of Delegation meeting in Berlin and is composed of ten members plus a Convenor and Vice-Convenor nominated by National Bodies and representing the membership from all SC 27 Working Groups. The MAG normally works electronically, but holds face-to-face meetings in conjunction with the WG meetings.

The Advisory Group functions purely in an advisory capacity to SC 27 Management. Any recommendations or proposals conveyed to SC 27 Management reflect a consensus outcome among MAG members. The Advisory Group is not empowered to make proposals directly to the SC 27 Plenary, except if granted prior authority by SC 27 Management.

3.6.1 MAG Accomplishments

The MAG presented a proposal to SC 27 Management for selection of a new name for the Committee by ballot, an issue where the SC 27 Plenary had been unable to reach consensus. After some modification by both SC 27 Management and the Wuhan Plenary, a ballot has been held.

3.6.2 MAG Deliverables

The MAG does not perform any standards development work itself and only produces recommendations to SC 27 Management.

3.6.3 MAG Risks, Opportunities and Issues

Following its first report to SC 27 Management in Wuhan, proposed topics for MAG investigation were approved. However, the MAG Convenor was advised of the costs and difficulties of changing existing procedures and the need to take this into account. For operational reasons requested by the Host it has been necessary to change the logistical arrangements for the second 2018 WG meetings at relatively short notice and this will provide an excellent opportunity for feedback to the MAG as to what is achievable in practice.

MAG has also been investigating additional topics like improvement of liaison management, registration and CRM processes, and improvement of communications.

3.7 SWG-T on Transversal Items

The SC 27 Special Working Group on Transversal Items (SWG-T) is an SC 27 internal administrative group created to handle SC 27 cross Working Group matters. In particular it provides a forum to allow WG convenors to review and discuss new work, originally just the content of any SC 27 New Work Item Proposals, but recently the discussions have been expanded to include a review of any new Terms of Reference for Working Group Study Periods. SWG-T maintains a list of key concepts and words used to help identify any new work that is transversal in nature. Once identified SWG-T often recommends collaboration between Working Groups to the SC 27 plenary.

3.7.1 SWG-T Accomplishment

SWG-T holds regular meetings and has hosted a number of cross working group external presentations, with the aim of allowing participation by experts of multiple different Working Groups. Examples of such external presentations have had as their topics, include: cloud computing, societal security and trusted virtual architectures.

3.7.2 SWG-T Deliverables

SWG-T does not perform any standards development work itself and only produces recommendations to SC 27 Plenary, for instance in the area of liaison process handling. SWG-T has been tasked to perform the editorial maintenance of the following SC 27 Standing Documents:

- SD14 -- Transversal item handling
- SD15 -- Scope alignment on SC 27 transversal items
- SD16 – Information security library
- SD17 – SC 27 Guide for editors

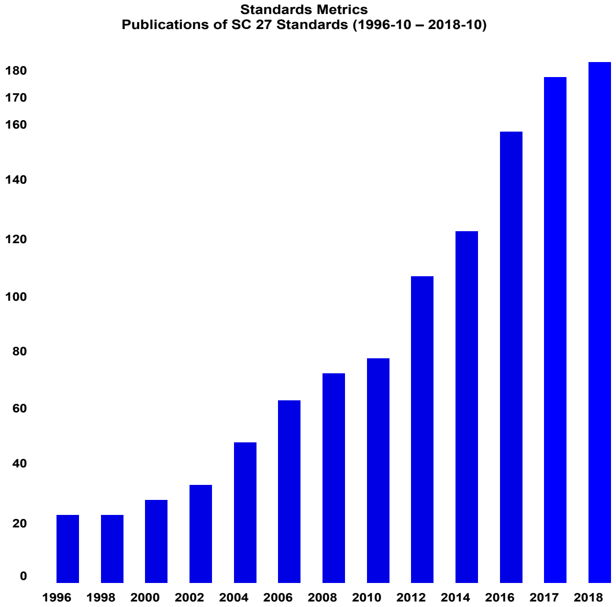
3.7.3 SWG-T Risks, Opportunities and Issues

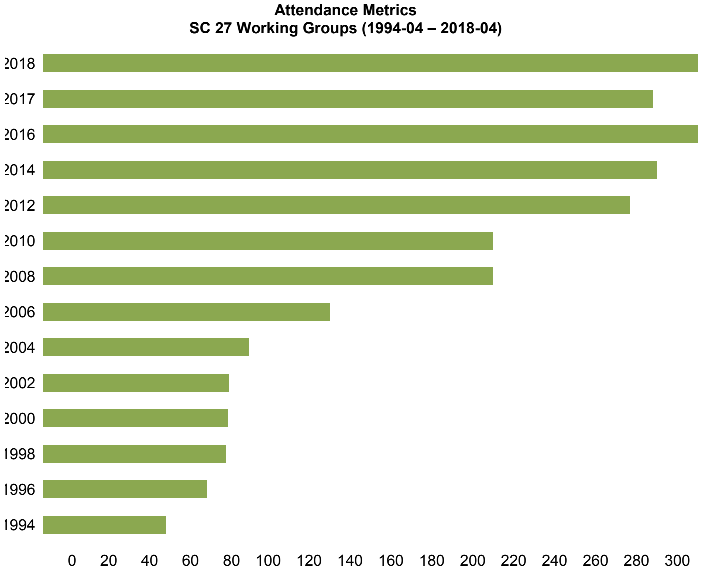
As SWG-T has the ability to review and bring together in a single forum all of the current and proposed new work of SC 27, SWG-T has the opportunity to identify and recommend a coordinated development process for SC 27. In order to further enable this SWG-T has also started to run a new work planning session once per year.

JTC 1/SC 27 DASHBOARD 2017

Performance Indicators

Systematic Reviews				Standards			
Year	Total Closed	Closed On time	% on time	Number Published	Avg time to Publish	# within timeframe	% within timeframe
2017	15	15	100%	19	44,68	3	20%
2018	5	5	100%	9	35,71	5	71%





New Work Items

- Information technology – Cybersecurity – Overview and concepts (ISO/IEC NP 27100)
- Big data security and privacy – Processes (ISO/IEC NP 27045)
- IT Security techniques – Requirements for the competence of IT security testing and evaluation laboratories (ISO/IEC NP TS 23532)
- Cybersecurity -- Guidelines for Internet Security (revision of ISO/IEC 27032:2012)
- Information technology – Security techniques – Security requirements for authentication using biometrics on mobile devices (ISO/IEC NP 27553)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC NP 27554)

Work Group Studies

- Utility of the Statement of Applicability (SoA)
- Future of IWA17:2014-12 (WG 1)
- Inclusion of Grain-128A in ISO/IEC standard
- Inclusion of Cross-domain Password-based authenticated key exchange in ISO/IEC standard
- Security properties, test and evaluation guidance for white box cryptography
- Security Reference Model for Industrial Internet Platform (SRM-IIP)
- Security and privacy for IoT-Domotics
- Privacy consideration in practical workflows
- Additional privacy-enhancing data de-identification standards