REPLACES: N16655

ISO/IEC JTC 1/SC 27

Information technology -- Security techniques

Secretariat: DIN, Germany

DOC TYPE: **other document (defined)**

TITLE: **SC 27 Business Plan and Dashboard , IT Security techniques for the period covered : October 2017 – September 2018**

SOURCE: **Walter Fumy, SC 27 Chairman**

DATE: 2017-08-23

PROJECT:

STATUS: **for submission to JTC 1**

ACTION ID: **Info**

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, SWG-T Convenor

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

NO. OF PAGES: 1 + 11 + 1 (Attachment 1)

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

ISO/IEC JTC 1/SC 27 N17590

BUSINESS PLAN FOR JTC 1/SC 27

Information technology – Security techniques

PERIOD COVERED: October 2017 – September 2018

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 150 publications, among them one of the three most popular standards within ISO.

Committee membership has increased from 18 P-members in 1990 to 55 P-members (plus 20 O-members) in 2017, 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 44 of the 29th SC 27 Plenary meeting in Hamilton, NZ, April 24-25, 2017.

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 2016, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:

- IEC 10116:2017-07 (4th edition), "Information technology — Security techniques — Modes of operation for an n-bit block cipher"
- ISO/IEC 10118-1:2016-10 (3rd edition), "Hash-functions -- Part 1: General"
- ISO/IEC 11770-4:2017-07 (2nd edition), "Key management — Part 4: Mechanisms based on weak secrets"
- ISO/IEC 11770-6:2016-10 (1st edition), "Information technology — Security techniques — Key management — Part 6: Key derivation"
- ISO/IEC TR 15446:2017-08 (3rd edition), "Guidance for the production of Protection Profiles and Security Targets"
- ISO/IEC 15946-5:2017-08 (2nd edition), "Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation"
- ISO/IEC 15952-1: 2016-11 (1st edition), "Secret sharing – Part 1: General"
- ISO/IEC 18031:2011/Amd.1:2017-02, "Random bit generation -- Amendment 1: Deterministic random bit generation"
- ISO/IEC 18367: 2016-12 (1st edition), "Cryptographic algorithms and security mechanisms conformance testing"
- ISO/IEC 18370-1:2016-11 (1st edition), "Blind digital signatures – Part 1: General"
- ISO/IEC 20009-4:2017-08 (2nd edition), "Anonymous entity authentication — Part 4: Mechanisms based on weak secrets"
- ISO/IEC 24759:2017-03 (3rd edition), "Test requirements for cryptographic modules"
- ISO/IEC 27003:2017-03 (2nd edition), "Information security management systems implementation – Guidance"
- ISO/IEC 27004: 2016-12 (2nd edition), "Information security management - Measurements"
- ITU-T X.1051 | ISO/IEC 27011:2016-12 (2nd edition) "Information security management guidelines for telecommunications organizations based on ISO/IEC 27001"
- ITU-T X.1058 | ISO/IEC 29151:2017-08 (1st edition), "Code of practice for personally identifiable information protection"
- ISO/IEC 27034-6:2016-10 (1st edition), "Application security -- Part 6: Case studies "
- ISO/IEC 27035-1:2016-11 (1st edition), "Information security incident management -- Part 1: Principles of incident management"

- ISO/IEC 27035-2:2016-11 (1st edition), "Information security incident management -- Part 2: Guidelines to plan and prepare for incident response"
- ISO/IEC 27036-4:2016-10 (1st edition), "Information security for supplier relationships -- Part 4: Guidelines for security of cloud services"
- ISO/IEC 27050-1:2016-11 (1st edition), "Electronic discovery - Part 1: Overview and concepts"
- ISO/IEC 29134:2017-06 (1st edition), "Guidelines for privacy impact assessment"

2.3 Resources

The last SC 27 Plenary meeting took place April 24 - 25 2017 in Hamilton, NZ and was attended by 75 delegates from 27 of the current 55 P-members.

The five SC 27 Working Groups held meetings April 18 - 22, 2017 in Hamilton, NZ, and October 23 – 27, 2016 in Abu Dhabi, United Arab Emirates. In both the Hamilton and Abu Dhabi meetings around 280 delegates attended the five SC 27 Working Groups.

The next set of Working Group meetings are scheduled for October 30 – November 3, 2017 in Berlin, Germany. The next SC 27 Plenary will take place April 23 - 24, 2017 in Wuhan, China and will be preceded by meetings of the five SC 27 Working Groups, April 16 - 20, 2018 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 9, WG 10, WG 11, SC 6, SC 7, SC 17, SC 22, SC 25, SC 31, SC 36, SC 37, SC 38, SC 40 and SC 41;
- within ISO including TC 46, TC 68, TC 176, TC 215, TC 251, PC 259, TC 262, TC 272, TC 292, ISO/PC 302, ISO/TC 307, 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, CEN/TC 377, CSA, ENISA, EPC, ETSI, FIRST, Global Platform, ICDPPC, IEEE, INLAC, INTERPOL, ISACA, $(ISC)^2$, ISA99, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, OASIS, OECD, OpenID Foundation, PICOS, PQCRYPTO, PRIPARE, SAFEcrypto, Small Business Standards, and WITDOM.

Currently SC 27 maintains 45 internal and 48 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 X.gpim | ISO/IEC 29151*, "Code of practice for the protection of personally identifiable information".

**Awaiting publication*

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 program 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 ISO/IEC 27003 (ISMS guidance), ISO/IEC 27004 "Information security management Monitoring, measurement, analysis and evaluation", ISO/IEC 27006 "International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems", ISO/IEC 27009 "Sector-specific application of ISO/IEC 27001 – Requirements" and ITU-T X.1051 | ISO/IEC 27011 "Information security management guidelines for telecommunications organizations based on ISO/IEC 27002".

WG1 also published Standing Document SD 27103 on "Cyber security and ISO and IEC standards", with a proposal to convert this into a TR in near term.

WG 1 has progressed work on the revised versions ISO/IEC 27007 "Guidelines for information security management systems auditing", ISO/IEC TR 27008 "Guidelines for auditors on ISMS controls" and ISO/IEC 27019 "Information security controls for the energy utility industry" with publication of all three expected by the end of 2017.

WG,1 is developing a new standard on the Competence Requirements for information security Management Professionals (ISO/IEC 27021) with expected publication by the end of 2017.

WG 1 has also embarked on the development of guideline on cyber insurance (ISO/IEC 27102). This will provide guidance on the use of insurance as a risk transfer option to

help an organization manage the impact of cyber security incidents.

Other deliverables include the Standing Documents SD 7 (Use of ISO/IEC family of standards in Governmental / Regulatory requirements) 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 the expected revisions of ISO/IEC 27000 (Overview and vocabulary), ISO/IEC 27002 (Code of practice for information security controls) and ISO/IEC 27005 (Information security risk management).

With growing interest in protection in cyberspace WG 1 has an on-going Study Period looking at various aspects of standardisation regarding cyber risk, cyber resilience and cyber security.

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 revision and maintenance IWA7.

3.1.2 WG 1 deliverables (this year and future)

The established market position of ISO/IEC 27001 and ISO/IEC 27002 as best selling 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.

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/PC302 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.

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

The established market position of ISO/IEC 27001 and ISO/IEC 27002 as best selling 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.

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/PC302 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 2016, ten standards have been published.

- ISO/IEC 14888-3, "Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms"
- ISO/IEC 10118-1, "Hash-functions – Part 1: General"
- ISO/IEC 11770-6, "Key management – Part 6: Key derivation"
- ISO/IEC 15946-1, "Cryptographic techniques based on elliptic curves – Part 1: General"
- ISO/IEC 18031/AMD1, "Random bit generation – Amendment 1"
- ISO/IEC 29192-4/AMD1, "Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques – Amendment 1"
- ISO/IEC 29192-5, "Lightweight cryptography – Part 5: Hash-functions"
- ISO/IEC 18370-1, "Blind digital signatures – Part 1: General"
- ISO/IEC 18370-2, "Blind digital signatures – Part 2: Discrete logarithm based mechanisms"
- ISO/IEC 19592-1, "Secret sharing – Part 1: General"

3.2.2 WG 2 deliverables

The following standards will be published in 2017.

- ISO/IEC 10116, "Modes of operation for an n-bit block cipher algorithm"
- ISO/IEC 10118-3, "Hash-functions – Part 3: Dedicated hash-functions"
- 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 19592-2, "Secret sharing – Part 2: Fundamental mechanisms"

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 2016:

- ISO/IEC 17825:2016-01 (1st edition), "Testing methods for the mitigation of non-invasive attack classes against cryptographic modules"
- ISO/IEC 18367:2016-12 (1st edition), "Cryptographic algorithms and security mechanisms conformance testing"
- ISO/IEC 19249 Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications

3.3.2 WG 3 deliverables

The following products have been, or are to be published, during 2017:

- ISO/IEC TR 15446:2017-08 (3rd edition), "Guidance for the production of Protection Profiles and Security Targets"
- ISO/IEC TS 19249 (1st edition), "Catalogue of architectural and design 3 principles for secure products, systems, and applications"
- ISO/IEC TS 19608 (1st edition), "Guidance for developing security and privacy functional requirements based on ISO/IEC 15408"
- ISO/IEC 19896-1 (1st edition), "Competence requirements for information security testers and evaluators -- Part 1: Introduction, concepts and general requirements"
- ISO/IEC 19896-2 (1st edition), "Competence requirements for information security testers and evaluators -- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
- ISO/IEC TS 20540 (1st edition), "Guidelines for testing cryptographic 3 modules in their operational environment"
- ISO/IEC 24759:2017-03 (3rd edition), " Test requirements for cryptographic modules"

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

WG 4 has updated its scope statement to more clearly reflect its scope. Th statement is as follows.

The scope 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 2016/2017:

- ISO/IEC 27033-6:2016-06 (1st edition), Network security – Part 6: Securing wireless IP network access
- ISO/IEC 27034-6:2016-10 (1st edition), Application security – Part 6: Case studies
- ISO/IEC 27036-4:2016-10 (1st edition), Information security for supplier relationships — Part 4: Guidelines for security of cloud services
- ISO/IEC 27050-1:2016-11 (1st edition), Electronic discovery – Part 1: Overview and concepts

3.4.2 WG 4 deliverables

The following products are expected to be published in 2017/2018:

- ISO/IEC 27034-3, Application security – Part 3: Application security

management process

- ISO/IEC 27034-5, Application security – Part 5: Protocols and application security controls data structure
- ISO/IEC 27050-3, Electronic discovery – Part 3: Code of practice for electronic discovery

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 and cloud computing.

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

- ISO/IEC 24760-3:2016-08 (1st edition), "A framework for identity management Part 3: Practice"
- ISO/IEC 29134:2017-06 (1st edition), "Guidelines for privacy impact assessment"
- ITU-T X.1085 (bhsm) | ISO/IEC 17922:2017-08 (probably) (1st edition) "Telebiometric authentication framework using biometric hardware security module" (awaiting publication)
- ITU-T X.1058 | ISO/IEC 29151:2017-08 (1st edition), "Code of practice for personally identifiable information protection"
- WG 5 Standing Document 2 – "Privacy references list"
- WG 5 Standing Document 4 – "Standards Privacy Assessment"

3.5.2 WG 5 deliverables

- ISO/IEC 24760-1:2011/Amd.1, "A framework for identity management – Part 1: Terminology and concepts – Amendment 1"
- ISO/IEC TS 29003, "Identity proofing"
- ISO/IEC 29100:2011/Amd.1, "Privacy framework – 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)

The upcoming of 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.

3.6 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.

3.6.1 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.

3.6.2 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

3.6.3 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.

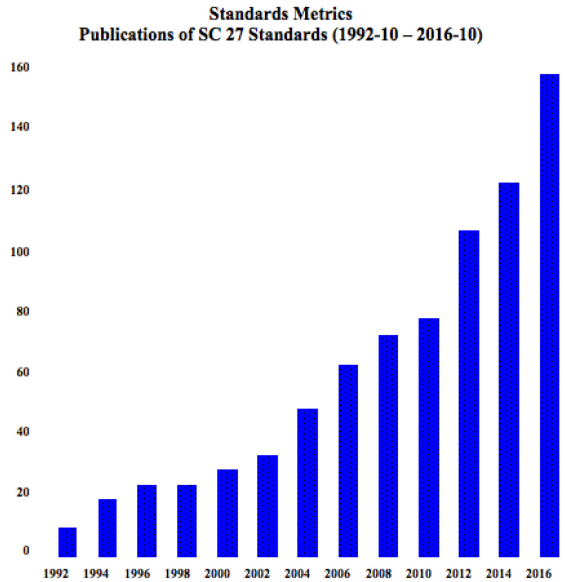
JTC 1/SC 27 DASHBOARD 2017

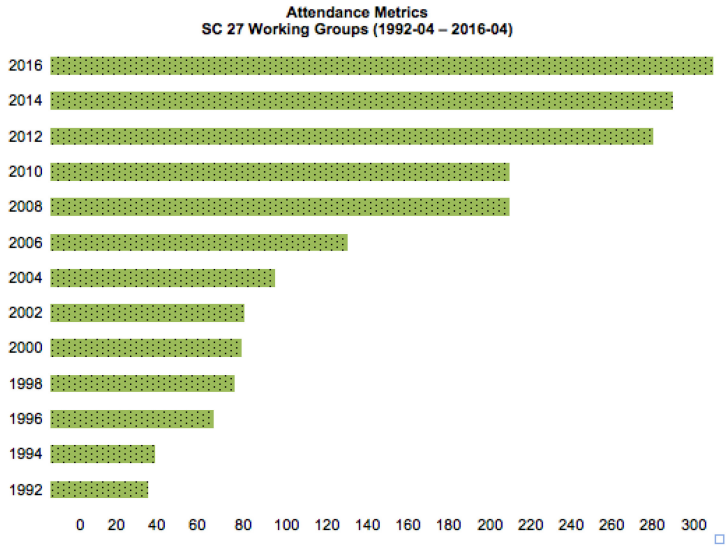
Performance Indicators

Systematic Reviews

Standards

Year	Total Closed	Closed On time	% on time	Number Published	Avg time to Publish	# within timeframe	% within timeframe
2016	18	18	100%	24	53,76		57,14%
2017	3		100%	10			





New Work Items

- Big Data Reference Architecture Part 4 – Security and privacy fabric
- Security guidelines for design and implementation of virtualized servers
- Privacy Engineering
- Criteria and methodology for security evaluation of biometric systems
- Anonymous entity authentication
- Enhancement to ISO/IEC 27001 for privacy management
- Lightweight cryptography – Part 6: Message authentication codes
- Anonymous entity authentication -- Part 3: Mechanisms based on blind signatures

Work Group Studies

- Cyber insurance guidelines
- Cyber resilience guidelines
- Broadcast authentication protocols
- Guidelines for Privacy in Internet of Things
- Guidelines for Security in Internet of Things
- ICT readiness for electronic discovery
- Information security guidance for PKI service providers
- Design specification for the revision of 27002, 27005 and 27014