ISO/IEC JTC 1/SC 27 **N19950**

**REPLACES:** N18950

**ISO/IEC JTC 1/SC 27**

**Information security, cybersecurity and privacy protection**

**Secretariat: DIN, Germany**

**DOC TYPE:** **business plan (open)**

**TITLE:** **SC 27 Business Plan Information security, cybersecurity and privacy protection for the period covered: October 2019 – September 2020**

**SOURCE:** **Andreas Wolf, SC 27 Chairman**

**DATE:** 2019-09-23

**PROJECT:**

**STATUS:** **for submission to JTC 1**

**ACTION ID:** **INFO**

**DUE DATE:**

**DISTRIBUTION:** P, O, L Members
L. Rajchel, JTC 1 Secretariat
J. Alcorta, ISO/CS (ITTF)
A. Wolf, SC 27 Chairman
L. Lindsay, 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 + 15 + 5 (Annex)

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627, [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 N19950

# BUSINESS PLAN FOR JTC 1/SC 27

## Information security, cybersecurity and privacy protection

## PERIOD COVERED: October 2019 – September 2020

### 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 48 P-members (plus 30 O-members) in 2019, 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 31st SC 27 Plenary meeting in Tel Aviv, Israel, 8th – 9th April 2019.

### 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 2018, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:

- ISO/IEC 9798-2:2019-06 (4th edition), IT Security techniques -- Entity authentication - Part 2: Mechanisms using authenticated encryption
- ISO/IEC 9798-3:2019-01 (3rd edition), IT Security techniques -- Entity authentication - Part 3: Mechanisms using digital signature techniques
- ISO/IEC 10118-3:2018-10 (4th edition), IT Security techniques -- Hash-functions -- Part 3: Dedicated Hash-functions
- ISO/IEC 11770-2:2018-10 (3rd edition), IT Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques

  ISO/IEC 14888-3:2018-11 (4th edition), IT Security techniques -- Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms
- ISO/IEC 19086-4:2019-01 (1st edition), Information technology – Cloud computing Service Level Agreement (SLA) framework -- Part 4: Components of security and of protection of PII (JOINT SC 27/SC 38 project)
- ISO/IEC TS 19608:2018-10 (1st edition), Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
- ISO/IEC 20543:2019-09 (1st edition), Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
- ISO/IEC 20889:2018-11 (1st edition), Privacy enhancing data de-identification techniques
- ISO/IEC 21878:2018-11 (1st edition), Information technology – Security techniques – Security guidelines for the design and implementation of virtualized servers
- ISO/IEC 24760-1:2019-05 (2nd edition), IT security and privacy -- A framework for identity management -- Part 1: Terminology and concepts
- ISO/IEC TS 27008:2019-01 (1st edition), Information technology -- Security techniques -- Guidelines for the assessment of information security controls (1st edition cancels and replaces ISO/IEC TR 27008)
- ISO/IEC 27018:2019-01 (2nd edition), Information technology – Security techniques -- Code of practice for PII protection in public clouds acting as PII processor
- ISO/IEC 27019:2017-10 (2nd edition) corrected 2019-08, Information technology — Security techniques — Information security controls for the energy utility industry
- ISO/IEC 27050-2:2018-09 (1st edition), Information technology – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery

- ISO/IEC 27102:2019-08 (1st edition), Information security management — Guidelines for cyber-insurance
- ISO/IEC TR 27550:2019-09 (1st edition), Privacy engineering for system life cycle processes
- ISO/IEC 27701:2019-08 (1st edition), Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines [this was developed as ISO/IEC 27552]
- ISO/IEC 29147:2018-10 (2nd edition), Information technology – Security techniques -- Vulnerability disclosure
- ISO/IEC 29192-6:2019-09 (1st edition), Information technology -- Lightweight cryptography -- Part 6: Message authentication codes (MACs)
- ISO/IEC 29192-7:2019-08 (1st edition), Information technology -- Lightweight cryptography -- Part 7: Broadcast authentication protocol
- ISO/IEC 30111:2019-09 (2nd edition), Information technology -- Security techniques -- Vulnerability handling processes

## 2.3 Resources

The last SC 27 Plenary meeting took place on April 8th – 9th 2019 in Tel-Aviv, Israel and was attended by 83 delegates from 31 of the current 48 P- and 30 O-members.

The five SC 27 Working Groups held meetings on 30th September – 4th October 2018 in Gjøvik, Norway and on 1st – 5th April 2019 in Tel-Aviv. In both the Gjøvik and Tel-Aviv meetings around 280 delegates attended the five SC 27 Working Groups.

The Joint Working Group 4 (JWG 4) also met in Tel Aviv. JWG 4 is a joint WG between ISO/TC 307 and JTC 1/ SC 27. Around 30 JWG 4 experts met in Tel Aviv.

The next set of Working Group meetings are scheduled for 14th – 18th October 2019 in Paris, France. The next SC 27 Plenary will take place on 27th and 28th April 2020 in Russia and will be preceded by meetings of the five SC 27 Working Groups, April 21st – 25th April 2020 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 JTC 1/WG 11, SC 6, SC 7, SC 17, SC 22, SC 25, SC 31, 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 292, ISO/PC 302, ISO/TC 307, ISO/TC 309, ISO/TC 314, ISO/PC 317, 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 13, CEN/TC 377, CEN/TC 428, CREDENTIAL, CSA, ENISA, EPC, ETSI, FIDO Alliance, FIRST, Global Platform, ICDPPC, IEEE, IFAA, INLAC, INTERPOL, ISACA, ISF, $(ISC)^2$, ISA99, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, OASIS, OECD, OpenID Foundation, PICOS, PQCRYPTO, PRIPARE, PRISMACLOUD, SAFECode, SAFEcrypto, Small Business Standards, TREsPASS.

Currently SC 27 maintains 48 internal and 49 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. In 2018, SC 27 has endorsed the creation of a Joint Working Group (JWG 4) with TC 307 to complement knowledge and standardization expertise in the domains of Blockchain Security, Identity and Privacy. 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 accreditation, auditing and certification standards, ISMS sector-specific controls, competence requirements for ISMS professionals and ISMS applied to protection in cyberspace. The complete SC 27/WG1 programme of work can be found described in SC 27 Standing Document SD11. 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 and Technical Specifications:

- ISO/IEC TS 27008:2019-01 (1st edition), Information technology -- Security techniques -- Guidelines for the assessment of information security controls (1st edition cancels and replaces ISO/IEC TR 27008)
- ISO/IEC 27019:2017-10 (2nd edition) corrected 2019-08, Information technology — Security techniques — Information security controls for the energy utility industry

WG 1 also published the 1st edition of the following deliverable:

- ISO/IEC 27102:2019-08 (1st edition), Information security management — Guidelines for cyber-insurance

### *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 27002 (WD3), Code of practice for information security controls (revision)
- ISO/IEC 27005 (WD), Information security rest management (revision)
- ISO/IEC 27006/AMD 1 (DAM), Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems – Amendment 1
- ISO/IEC 27009 (DIS), Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 – Requirements (revision)
- ISO/IEC 27013 (WD), Information technology -- Security techniques -- Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (revision)
- ISO/IEC 27014 (CD), Information technology -- Security techniques -- Governance of information security (revision)
- ISO/IEC 27021/AMD 1 (PDAM), Information technology -- Security techniques -- Competence requirements for information security management systems professionals -- Amendment 1
- ISO/IEC 27022 (WD), Information technology -- Security techniques -- Guidance on ISMS processes
- ISO/IEC 27100 (WD), Information technology -- Cybersecurity – Overview and concepts
- ISO/IEC TS 27101 (WD), Information technology -- Security techniques -- Cybersecurity Framework development guidelines

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).

Finally, WG 1 is expected to embark in the near future on work in the field of sector specific certification requirements as en extension to ISO/IEC 27006.

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

The established market position and global outreach of ISO/IEC 27001 and ISO/IEC 27002 as bestselling ISO/IEC standards in information security management is an outstanding achievement. Both these standards provide a common international language that facilitates many opportunities for growth and harmonisation across all market sectors, especially to address the diverse and continual increase in cyber risks and to support cyberspace governance. 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, the WG 1 programme of work attracts the attention of other ISO and IEC TCs/SCs 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 ISO CASCO and IEC/CAB concerning several aspects of MSS accreditation, 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*

Since October 2018, the following standards have been published:

- ISO/IEC 9798-2:2019-06 (4th edition), IT Security techniques -- Entity authentication - Part 2: Mechanisms using authenticated encryption
- ISO/IEC 9798-3:2019-01 (3rd edition), IT Security techniques -- Entity authentication - Part 3: Mechanisms using digital signature techniques
- ISO/IEC 10118-3:2018-10 (4th edition), IT Security techniques -- Hash-functions -- Part 3: Dedicated Hash-functions
- ISO/IEC 11770-2:2018-10 (3rd edition), IT Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques

ISO/IEC 14888-3:2018-11 (4th edition), IT Security techniques -- Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms

- ISO/IEC 29192-6:2019-09 (1st edition), Information security -- Lightweight cryptography -- Part 6: Message authentication codes (MACs)
- ISO/IEC 29192-7:2019-08 (1st edition), Information security -- Lightweight cryptography -- Part 7: Broadcast authentication protocol

WG 2 is progressing the development of a number of cybersecurity specific standards including:

### *3.2.2 WG 2 deliverables*

The following standards will be published in 2019-10/2020-09 or in the subsequent cycle:

- ISO/IEC 9797-2 (CD), Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function (revision)
- ISO/IEC 9797-3/AMD 1 (DAM), Information technology -- Security techniques -- Message authentication codes (MACs) - Part 3: Mechanisms using a universal hash-function -- Amendment 1
- ISO/IEC 11770-4/AMD1 (FDAM) , Information technology -- Security techniques -- Key management – Part 4: Mechanisms based on weak secrets – Amendment 1
- ISO/IEC 11770-4/AMD1 (PDAM) , Information technology -- Security techniques -- Key management – Part 4: Mechanisms based on weak secrets – Amendment 2
- ISO/IEC 11770-5 (CD), IT Security techniques -- Key management – Part 5: Group key management
- ISO/IEC 13888-1 (CD), Security, cybersecurity and privacy protection — Non-repudiation -- Part 1: General (revision)
- ISO/IEC 13888-3 (CD), Security, cybersecurity and privacy protection — -- Non-repudiation - Part 3: Mechanisms using asymmetric techniques (revision)
- ISO/IEC 18032 (DIS), Information technology — Security techniques — Prime number generation (revision)
- ISO/IEC 18033-1 (CD), Information technology — Security techniques — Encryption algorithms — Part 1: General (revision)
- ISO/IEC 18033-4/AMD 1 (PDAM), Information technology -- Security techniques – Encryption algorithms -- Part 4: Stream ciphers --Amendment 1: ZUC
- ISO/IEC 19772/AMD 1 (FDAM), Information technology — Security techniques — Authenticated encryption – Amendment 1
- ISO/IEC 20009-3 (CD), Information security — Anonymous entity authentication — Part 3: Mechanisms based on blind signatures
- ISO/IEC 23264-1 (CD), Information technology security techniques – Redaction of authentic data – Part 1: General

- ISO/IEC 29192-2 (2nd edition), Lightweight cryptography – Part 2: Block ciphers (will be merged with 29192-2/AMD 2)

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

Post-quantum cryptography is one of emerging technologies. WG 2 thinks it is too early to standardize it, but is now producing a standing document WG 2 SD8 (Post-quantum cryptography) for the preparation of standardization. WG 2 SD8 currently consists of six parts:

- Part 1: General post-quantum & motivation
- Part 2: Hash-based signatures
- Part 3: Lattice-based cryptography
- Part 4: Coding-based encryption
- Part 5: Multivariate-based signatures
- Part 6: Isogeny-based encryption

## 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 2018-10/2019-09 or in the subsequent cycle:

- ISO/IEC TS 19608:2018-10 (1st edition), Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
- ISO/IEC 20085-1:2019-09 (1st edition), IT Security techniques -- 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 20543:2019-09 (1st edition), Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
- ISO/IEC 29147:2018-10 (2nd edition), Information technology – Security techniques -- Vulnerability disclosure

### *3.3.2 WG 3 deliverables*

The following products have been, or are to be published, during 2019-10/2020-09 or in the subsequent cycle:

- ISO/IEC 15408-1 (CD), IT Security techniques – Evaluation criteria for IT security —
    - Part 1: Introduction and general model (revision)
    - Part 2: Part 2: Security functional components (revision)
    - Part 3: Security assurance components (revision)
    - Part 4: Framework for the specification of evaluation methods and activities
    - Part 5: Pre-defined packages of security requirements
- ISO/IEC 18045 (CD), IT Security techniques – Methodology for IT security evaluation (revision)
- ISO/IEC 19989-1 (DIS), Security techniques -- Criteria and methodology for security evaluation of biometric systems –
    - Part 1: Framework
    - Part 2: Biometric recognition performance
    - Part 3: Presentation attack detection
- ISO/IEC 20897-1 (DIS), Security requirements and test methods for physically unclonable functions for generating non-stored security parameters — Part 1: Security requirements
- ISO/IEC 20085-2 (DIS), Information technology -- IT Security techniques Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules -- Part 2: Test calibration methods and apparatus
- ISO/IEC 30111 (FDIS) (2nd edition), Information technology -- Security techniques -- Vulnerability handling processes

### *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 2018-10/2019-09:

- ISO/IEC 19086-4:2019-01 (1st edition), Information technology – Cloud computing – Service Level Agreement (SLA) framework – Part 4: Components of security and of protection of PII
- ISO/IEC 21878:2018-11 (1st edition), Information technology – Security techniques – Security guidelines for the design and implementation of virtualized servers
- ISO/IEC 27050-2:2018-09 (1st edition), Information technology – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery

### *3.4.2 WG 4 deliverables*

The following products are expected to be published in 2019-10/2020-09 or in the subsequent cycle:

- ISO/IEC 20547-4 (CD), Information technology -- Big data reference architecture – Part 4: Security and privacy
- ISO/IEC 27034-4 (CD), Information technology – Application security -- Part 4: Validation and verification
- ISO/IEC 27035-3 (CD), Information technology -- Information security incident management -- Part 3: Guidelines for ICT incident response operations
- ISO/IEC 27050-1 (FDIS) (2nd edition), Information technology — Electronic discovery — Part 1: Overview and concepts
- ISO/IEC 27050-3 (FDIS) (2nd edition), Information technology – 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 big data, cybersecurity and Internet of Things (IoT) is rapidly growing. As such, more and more projects are being 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. An example of this is the close collaboration with ISO TC 292, Security and resilience, on Information and communication technology readiness for business continuity.

## 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 2018-10/2019-09

- ISO/IEC 20889-2018-11 (1st edition), Privacy enhancing data de-identification techniques
- ISO/IEC 24760-1:2019-05 (2nd edition), IT security and privacy -- A framework for identity management -- Part 1: Terminology and concepts
- ISO/IEC TR 27550:2019-09 (1st edition), Privacy engineering for system life cycle processes
- ISO/IEC 27701:2019-08 (1st edition), Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines [this was developed as ISO/IEC 27552]
- 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 2019-10/2020-09 or in the subsequent cycle:

- ISO/IEC 24761 (2nd edition), Authentication context for biometrics
- ISO/IEC 27551 (CD), Information technology -- Security techniques – Requirements for attribute-based unlinkable entity authentication
    - ISO/IEC 27570 (PDTS), Information technology -- Security techniques – Privacy guidelines for smart cities
    - ISO/IEC 29184 (DIS), Information technology -- Online privacy notice and consent

### *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 continue to be very 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 31700, originally 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, an exercise, that is practised for the first time on October 2019 in Paris. There will be a joint meeting between WG 5 and PC 317/WG 1 on the Saturday after the SC 27 WG meetings. Monday till Wednesday after the joint meeting PC 317/WG 1 will be meeting.

## 3.6 ISO/TC 307-JTC 1/SC 27/JWG 4 – Blockchain and distributed ledger technologies and IT Security techniques

The newly formed JWG 4 has started its activities in 2018. This JWG is under the administrative responsibility of TC 307. Objective of this JWG is to produce Standards and Technical Reports in the domain of Blockchain Identity, Security and Privacy.

### *3.6.1 JWG 4 deliverables*

The following products are expected to be published in 2019-10/2020-09 or in the subsequent cycle:

- ISO/DTR 23244, Privacy and personally identifiable information protection considerations
- ISO/DTR 23245, Security risks, threats and vulnerabilities

### *3.6.2 JWG 4 strategies/risks/opportunities/lessons learned (if any)*

This Joint WG was created to leverage different expertise and competences to create a synergy among Blockchain experts and Security, Identity and Privacy experts. Managing a JWG can be more challenging than a regular WG. For this purpose, two Convenors have been appointed (one from TC 307 and a co-convener from SC 27).

In the past year, this JWG have seen an increase both in membership and active participation. The JWG is also working on refining its Programme of Work to answer to the need for standardization in Security, Identity and Privacy for Blockchain.

## 3.7 Management Advisory Group (MAG)

The SC 27 Management Advisory Group (MAG) is a new internal administrative function 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.

The internal discussions within the MAG are kept private to MAG members.

### *3.7.1 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 was held.

The MAG produced, distributed and analysed a questionnaire covering differing procedures within SC 27 Working Groups for the processing of documents at Committee Draft and higher. In consequence it will recommend to SC 27 Management a number of harmonization measures.

### *3.7.2 MAG Deliverables*

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

### *3.7.3 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 through the MAG as to what is achievable in practice.

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

## 3.8 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.

### *3.8.1 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.

### *3.8.2 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
- SD19 – Risk management resource library

### *3.8.3 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 Update
# Information security, cybersecurity and privacy protection

**Andreas Wolf**

**November 2019**

# Highlights

- The new cooperation activity is gaining momentum: ISO/TC 307/JWG 4: Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG on Blockchain and distributed ledger technologies and IT Security techniques
- Constantly increasing attraction to the participating experts and their National Bodies: 1446 registered experts
- 78 Standards currently under development, 15 published in the first 9 months of 2019
- Eagerly anticipated: ISO/IEC 27701: Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

# Challenges

Today, SC 27 is faced with

- Growing complexity of technologies in an increasing number of IT application fields with security needs,
- Increasing coverage of IT to virtually all application domains,
- An increasing market need for comparability of security properties of products and systems, this includes scalable and lower effort approaches, and
- Growing importance of privacy aspects including the need for comparability and applicability in many regional and national legal contexts.

# Plans

In the near future, SC 27 wants

- To improve the visibility of SC 27 products in other standardization entities, in particular in IEC,
- To modify the organizational structure of SC 27 in order to allow
  - Faster responses to requests from liaising organizations and
  - Improved awareness within SC 27 on relevant new technological and societal trends, and
- To develop continuously and in time high quality standards according to the market needs.


ISO
JTC 1
IEC
INFORMATION TECHNOLOGY STANDARDS