ISO/IEC JTC 1 **N 14904**

ISO/IEC JTC 1 "Information technology"
Secretariat: **ANSI**
Committee Manager: **Rajchel Lisa Mrs.**

SC 27 Business Plan 2020

Document type	Related content	Document date	Expected action
General document / Other		2020-09-11	**COMMENT/REPLY** by 2020-11-02

Description

This document is circulated for review and consideration at the November 2020 virtual JTC 1 plenary

ISO/IEC JTC 1/SC 27 **N 20990**

ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection"
Secretariat: **DIN**
Committee Manager: **Passia Krystyna Mrs**

JTC 1/SC 27 Business Plan for period Oct 2020 – Sept 2021

Document type	Related content	Document date	Expected action
Other		2020-09-03	**INFO**

Description

This document is circulated for information.

ISO/IEC JTC 1/SC 27 N20990

Business Plan for JTC 1/SC 27

Information security, cybersecurity and privacy protection

Period covered: October 2020 – September 2021

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 47 P-members (plus 33 O-members) in 2020, 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 6 of JTC 1 Virtual Meeting, 23-25 June 2020.

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 Communications and Outreach

SC 27 is engaged in many communication and outreach activities, managed by the Communications Officer. The objectives of external communication in SC 27 are:

- Achieve high levels of recognition, support and acceptance of the work of SC 27 by raising awareness of the committee and its work with the wider stakeholder communities;
- Develop and publish external communications for SC 27 to complement and supplement information published by ISO;
- Inform and encourage increased participation of experts in the work of the committee by effective communication of SC 27 activities and opportunities;
- Increase the use of the standards (and other documents) developed by the committee by increasing public knowledge of their application and value;
- To assist all elements of the SC 27 community to provide the comprehensive, understandable effective communications internally and externally.

SC 27 works together with ISO/CS, JTC 1/AG01 (Communications Advisory Group) and AG10 (Outreach) and other internal groups involved with communications.

Important target audiences and stakeholders for this work are:

- International and national enterprises;
- Business and service professionals
  - Utilities, healthcare, finance and insurance, IT sector
  - Accreditation, certification, testing and evaluation bodies
  - Business associations, alliances, forums
  - Professionals – consultants, advisors
- National/Federal/Provincial/State or Regional Government Agencies
- Academia and Research Institutions

- Non-government organizations
  - Standards Organizations/NSBs
  - International Organizations (e.g. OECD, INTERPOL)
- Media

Over the last 12 months the communication and outreach activity has, included(i) engaged with ISO and IEC in producing a number of articles and press releases, (ii) revision of the JTC 1 website pages relating to SC 27, and (iii) various workshops and seminars. The Communications Officer ran a Webinar (July 2020) for ISO and UNIDO on ISO/IEC 27001 family of standards and the cyber challenges of COVID-19. The SC 27 standing document SD 11 and its corporate presentation annual edition was released. On the 17th September SC 27 together with the Polish NB (PKN) has a one-day Web-based Conference on the future of cybersecurity standards.

2.3 Accomplishments

2.3.1 Publications

Since October 2019, the following International Standards, Technical Specifications, Technical Reports and Amendments have been published:

- ISO/IEC 9797-3:2011/Amd.1:2020 – Information technology — Security techniques — Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function — Amendment 1
- ISO/IEC 13888-1:2020-09 (4th edition) — Information security — Nonrepudiation — Part 1: General
- ISO/IEC 13888-3:2020-09 (3rd edition) — Information security — Nonrepudiation — Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 18033-4:2011/AMD 1:2020-08 — Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers — Amendment 1: ZUC
- ISO/IEC 20085-1:2019-10 (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 20085-2:2020-03 (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 2: Test calibration methods and apparatus
- ISO/IEC 20543:2019-10 (1st edition) — Information technology — Security techniques — Test and analysis methods for random bit generators

within ISO/IEC 19790 and ISO/IEC 15408

- ISO/IEC 24761:2019-10 (2nd edition) — Information technology — Security techniques — Authentication context for biometrics
- ISO/IEC 27007:2020-01 (2nd edition) — Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
- ISO/IEC 27009:2020-05 (2nd edition) — Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27050-1:2019-11 (2nd edition) — Information technology — Electronic discovery — Part 1: Overview and concepts
- ISO/IEC 27050-3:2020-01 (2nd ed.) – Information technology -- Electronic discovery -- Part 3: Code of practice for electronic discovery
- ISO/IEC 29184:2020-06 (1st edition) — Information technology — Online privacy notices and consent
- ISO/IEC 29192-2:2019-11 (2nd edition) — Information security — Lightweight cryptography — Part 2: Block ciphers
- ISO/IEC 30111:2019 (2nd edition) -- Information technology -- Security techniques -- Vulnerability handling processes

2.4 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.

In the period October 2019 until April 2020, the five SC 27 Working Groups met twice physically on 14th – 18th October 2019 in Paris, France and virtually on 20th – 24th April 2020. In both the Paris and virtual meetings, around 280 delegates attended the five SC 27 Working Groups.

The Joint Working Group 4 (JWG 4) also met also virtually on 28th and 30th April 2020. JWG 4 is a joint WG between ISO/TC 307 and JTC 1/ SC 27. Around 30 JWG 4 experts participated in the virtual April 2020 meeting.

The next set of Working Group meetings is scheduled to be held virtually on 12th – 16th September 2020, followed by a virtual Plenary on September 18th – 19th.

The following SC 27 Plenary is scheduled for April 2021 (exact date TBD) in Sankt Petersburg, Russian Federation and will be preceded by meetings of the five SC 27 Working Groups, at the same location, under the assumption that physical meetings will be possible again until then.

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 the following SC 27 Advisory Groups:

- Chairman‘s Advisory Group
- Advisory Group on Strategy (AG-S)
- Advisory Group on Operations (AG-O) and
- Advisory Group on Concepts and Terminology (AG-CT)

The Special Working Group on Transversal Items (SWG-T) was disbanded.

2.5 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, JTC 1/WG 13, SC 6, SC 7, SC 17, SC 22, SC 25, SC 29, 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 SM2TF, 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 224/WG 18, CEN/TC 377, CEN/TC 428, CREDENTIAL, CSA, ENISA, EPC, ETSI, Functional ENcryption TEChnologies (FENTEC), FIDO Alliance, FIRST, Global Platform, IAF, ICDPPC, IEEE, IFAA, INLAC, INTERPOL, ISACA, ISF, (ISC)2, ISA99, ISCI, ISF, ITU-T, Kantara Initiative, MasterCard, OASIS, OECD, OpenID Foundation, PICOS, PQCRYPTO, PRIPARE, SAFECode, SAFEcrypto, Small Business Standards, TREsPASS.

Currently SC 27 maintains 51 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.

2.5.1 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'.

2.5.2 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".

2.5.3 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.

2.5.4 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.

2.5.5 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 27000 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 cybersecurity. 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 27006:2015/Amd 1:2020 Requirements for bodies providing audit and certification of information security management systems — Amendment 1
- ISO/IEC 27007: 2020 (3rd edition) Guidelines for information security management systems auditing
- ISO/IEC 27009: 2020 (2nd edition) Sector-specific application of ISO/IEC 27001 — Requirements

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

- ISO/IEC TS 27101 (1st edition), Information technology -- Security techniques -- Cybersecurity Framework development guidelines
- 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 (CD2), Code of practice for information security controls (revision)
- ISO/IEC 27005 (CD), Information security rest management (revision)
- ISO/IEC 27013 (CD), Information technology -- Security techniques -- Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (revision)
- ISO/IEC 27014 (FDIS), Information technology -- Security techniques -- Governance of information security (revision)
- ISO/IEC 27022 (CD2), Information technology -- Security techniques -- Guidance on ISMS processes
- ISO/IEC 27100 (CD), Information technology -- Cybersecurity – Overview and concepts

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 PWIs on (i) guidelines for cybersecurity insurance and

(ii) cyber education and training.

Finally, WG 1 is expected to embark in the near future on work in the field of sector specific certification requirements as an 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 – ISO/IEC 27001 is ranked third in the ISO survey of Management System Standards (MSSs). Both these standards provide a common international language that facilitates many opportunities for growth and harmonization 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 standardization.

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 2019, the following standards have been published:

- ISO/IEC 9797-3/AMD1:2020-02, Information security -- Message authentication codes (MACs) - Part 3: Mechanisms using a universal hash-function – Amendment 1

- ISO/IEC 29192-2:2019-11 (2nd edition), Information security -- Lightweight cryptography -- Part 2: Block ciphers

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 2020-10/2021-09 or in the subsequent cycle:

- ISO/IEC 9797-2 (DIS), Information security -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function (revision)
- ISO/IEC 10116/AMD1 (DAM), Information security – Modes of operations for an n-bit block cipher – Amendment 1
- ISO/IEC 10118-1/AMD1 (DAM), Information security – Hash-functions – Part 1: General – Amendment 1
- ISO/IEC 11770-4/AMD2 (DAM) , Information technology -- Security techniques -- Key management – Part 4: Mechanisms based on weak secrets – Amendment 2
- ISO/IEC 11770-5 (DIS), Information security -- Key management – Part 5: Group key management (revision)
- ISO/IEC 11770-7 (DIS), Information security -- Key management – Part 7: Group key management
- ISO/IEC 13888-1 (FDIS), Information security – Non-repudiation -- Part 1: General (revision)
- ISO/IEC 13888-3 (FDIS), Information security -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques (revision)
- ISO/IEC 15946-5 (CD), Information security – Cryptographic techniques based on elliptic curve – Part 5: Elliptic curve generation (revision)
- ISO/IEC 18014-2 (CD), Information security – Time-stamping services – Part 2: Mechanisms producing independent tokens (revision)
- ISO/IEC 18032 (FDIS), Information security techniques — Prime number generation (revision)
- ISO/IEC 18033-1 (CD), Information security -- Encryption algorithms — Part 1: General (revision)
- ISO/IEC 18033-4/AMD 1 (DAM), Information security – Encryption algorithms -- Part 4: Stream ciphers --Amendment 1

- ISO/IEC 18033-5/AMD 1 (DAM), Information security -- Encryption algorithms – Part 5: Identity-based ciphers – Amendment 1
- ISO/IEC 19772 (FDIS), Information security — Authenticated encryption (minor revision)

- ISO/IEC 20009-3 (CD), Information security — Anonymous entity authentication — Part 3: Mechanisms based on blind signatures
- ISO/IEC 20008-2/AMD1 (DAM), Information security – Anonymous digital signatures – Part 2: Mechanisms using a group public key – Amendment 1
- ISO/IEC 23264-1 (DIS), Information security-- Redaction of authentic data – Part 1: General
- ISO/IEC 23264-2 (CD), Information security -- Redaction of authentic data – Part 2: Redactable signature schemes based on asymmetric mechanisms

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

WG 2 SD8 is currently publicly available from the SC 27 public website at www.din.de/go/jtc1sc27 / Downloads.

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:

- security evaluation criteria;
- methodology for application of the criteria;

- security functional and assurance specification of IT systems, components and products;
- testing methodology for determination of security functional and assurance conformance;
- administrative procedures for testing, evaluation, certification, and accreditation schemes.

3.3.1 WG 3 accomplishments

The following products were published during 2019-10/2020-09 or in the subsequent cycle:

- ISO/IEC 20085-2:2020-03 (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 2: Test calibration methods and apparatus
- ISO/IEC 30111:2019-10 (2nd edition), Information technology -- Security techniques -- Vulnerability handling processes

3.3.2 WG 3 deliverables

The following products have been, or are to be published, during 2020-10/2021-09 or in the subsequent cycle:

- ISO/IEC 15408-1 (DIS), 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 (DIS), IT Security techniques – Methodology for IT security evaluation (revision)
- ISO/IEC 19989-1 (FDIS), 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

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

WG 3 is completing 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 2021, 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:

- ICT security operations (for example readiness, continuity, incident and event management, investigation)
- Information lifecycle (for example creation, processing, storage, transmission and disposal)
- Organizational processes (for example design, acquisition, development and supply)
- Security aspects of Trusted services (for example in the provision, operation and management of these services)
- 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 2019-10/2020-09:

- ISO/IEC 27050-1:2019 (2nd edition), Information technology – Electronic discovery – Part 1: Overview and concepts
- ISO/IEC 27050-3:2020 (2nd edition), Information technology – Electronic discovery – Part 3: Code of Practice for electronic discovery

3.4.2 WG 4 deliverables

The following products are expected to be published in 2020-10/2021-09 or in the subsequent cycle:

- ISO/IEC 20547-4 (FDIS), Information technology – Big data reference architecture – Part 4: Security and privacy
- ISO/IEC 27034-4 (FDIS), Information technology – Application security – Part 4: Validation and verification
- ISO/IEC 27035-3 (FDIS), Information technology – Information security incident management – Part 3: Guidelines for incident response operations
- ISO/IEC 27050-4 (DIS), Information technology – Electronic discovery – Part 4: Technical readiness

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 (ISO/IEC JTC 1/SC 7 and ISO/IEC JTC 1/SC 42), and Internet of Things (ISO/IEC JTC 1/SC 25 and ISO/IEC JTC 1/SC 41). WG 4 especially involves relevant committees by requesting co-editors from these committees. An example of this is the collaboration with ISO TC 292, Security and resilience, on Information and communication technology readiness for business continuity.

WG 4 also has close relationships with its liaisons. An examples is Small Business Standards (SBS) who provided a co-editor for ISO/IEC 27035-1, Information technology – Information security incident management – Part 1: Principles of incident management.

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 2019-10/2020-09

- ISO/IEC 24761:2019-10 (2nd edition) — Information technology — Security techniques — Authentication context for biometrics
- ISO/IEC 29184:2020-06 (1st edition) — Information technology — Online privacy notices and consent
- WG 5 Standing Document 2 – Privacy references list

3.5.2 WG 5 deliverables

The following products are expected to be published in 2020-10/2021-09 or in the subsequent cycle:

- ISO/IEC 27555 (CD) Guidelines on personally identifiable information deletion
- ISO/IEC 27556 (CD) User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences
- ISO/IEC 27551 (DIS), Information technology -- Security techniques – Requirements for attribute-based unlinkable entity authentication
- ISO/IEC 27570 (DTS), Information technology -- Security techniques – Privacy guidelines for smart cities
- ISO/IEC 27555 (CD) Guidelines on personally identifiable information deletion
- ISO/IEC 27556 (CD) User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences

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

Privacy and identity management legislation around the world is relying more and more on standards, asking for more standards to implement the respective regulations and best practices. This is an opportunity, as more and more WG 5 products are receiving attention and are being sold and used. Moreover the group is attracting more volunteers. The trend is a challenge, as the group is growing and the privacy work elsewhere is also intensified. So WG 5 is continuing to maintain many liaisons. Especially liaisons with research projects continue to be very successful: Relevant innovative content was contributed and more volunteers were kept for WG 5 work 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 was practiced for the first time in October 2019 in Paris. There was 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 was meeting. This setting proved successful in generating mutual understanding and improving the quality of the work. So it is planned to be repeated in the near future with even the hosting of all SC 27 WGs offered from the PC 317 volunteer base. However the restrictions on physical meetings due to COVID-19 forced to postpone these activities.

In general the (COVID-19 forced) experiences with virtual meetings don't give reason for much enthusiasm. While virtual meetings can be arranged easily compared to physical ones their effectiveness is lower, as they don't enable the full spectrum of interaction the standardisation process needs, especially in an in interdisciplinary field and for innovative approaches. The formal process steps get executed, but deeper exchanges don't really happen, especially if experts had not met physically before. Additionally, "webinar" fatigue is spreading.

Moreover the restrictions on meeting time per day (induced by the need to cover all time zones) reduce what can be achieved in a meeting day.

The concept to spread meetings over more meeting days is of limited value especially for those experts who are not working fulltime in standardisation and need to synchronise their international volunteer work for a committee with the respective national work, the work for other committees, and last but not least the work they get paid for.

In this context, it has not been helpful that the ISO Central Secretariat abandoned Comment Resolution Meetings that were held by WGs for SCs making use of national delegations to handle comments accompanying national body votes on ballots at Committee or Enquiry stage. Comments accompanying national body votes on ballots at Committee or Enquiry stage result from national decision processes, often by compromise in the respective National Bodies. However in the WGs the experts are supposed to act only in their expert capacity (neutral wrt National Body positions) while they are trying to resolve comments that often require negotiations and compromises between National Bodies. If there are no national delegations in a meeting that can make decisions and agree on compromises the reactions on compromise proposals are delayed till the respective national position is found, possibly in a subsequent national meeting. It cannot be assumed, that National Bodies arrange for mirror committee meetings, when only experts are in a WG meeting. This holds especially when expert meetings are spread over the calendar year and not focussed on e.g. two occasions per year. This lack of opportunity to synchronise nationally limits the quality of the compromises that can be achieved, when a WG is working on Committee or Enquiry Stage comments. Either experts are very reluctant to agree on a compromise, as they lack the national feedback from those colleagues with whom they negotiated the respective comment nationally or they don't care to defend the national comment, as they don't represent "their" National Body. Even the expectation, that a National Body comment may not be considered very much, if it is not defended by a national representative is less legitimate in an expert meeting, as there are no delegations that can be held "responsible" for a comment. None of the scenarios is helpful to generate a sustainable consensus in the WG meeting that is preserved in the next National Body ballot receiving more approval votes.

In summary the current restrictions are hindering the work of WG 5 at a time, when its results are needed, expected and respected more than ever before. The respective committees in JTC 1 and ISO need to make wise decisions considering the actual processes that are needed to generate sustainable consensus efficiently. They also need to enable SCs and WGs to define their way of work in a way that considers their requirements for success.

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

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 leveraging the expertise of the two parents committees.

3.6.1 JWG 4 deliverables

The following products are expected to be published in 2020-10/2021-09 or in the subsequent cycle:

- ISO/TR 23249 (has replaced ISO/TR 23246), Overview of existing DLT systems for identity management

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

This Joint WG was created to leverage different expertise and competences from the two parents committees 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 co-convenors have been appointed (one from TC 307 and one from SC 27).

In the past year, this JWG has 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. The JWG has a unique capability of collaborating with the working groups of both committees in order to ensure compatibility with existing standards developed in SC 27 and adaptation to the specificities of blockchain.

3.7 Management Advisory Group (MAG)

The SC 27 Management Advisory Group (MAG) is an 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 normally 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

During this period MAG presented a proposal to SC 27 Management for improvement of meetings management and Working Groups organization in order to improve SC27 efficiency. MAG also prepared a form to improve liaison management. These proposals were discussed with the SC27 Management team.

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 or food for thought for SC 27 Management.

3.7.3 MAG Risks, Opportunities and Issues

MAG is currently working on improvement of SC27 functioning given the probable growing place of virtual meetings in the future. MAG's current intention is to propose more flexibility and proactivity in SC27 management. MAG is currently working in an environment where there is forced rapid change to SC27 processes - both due to Corona virus but also changes in ISO CS policies and the tools made available for committee member use. A strategic direction will again be important once SC27 has survived its current short-term issues.

3.8 Chairman's Advisory Group (CAG)

3.8.1 CAG Deliverables

CAG does not develop deliverables itself. CAG supports the SC 27 Chair in leading SC 27 between the Plenaries. CAG shall give recommendations to the Chair and the Committee Manager on all decisions which can't be postponed until the next Plenary and/or which are unsuitable for a Letter Ballot. CAG in particular takes part in organizing the SC 27 meetings. CAG supports the SC 27 Chair and SC 27 experts handling liaisons to other organizations if necessary and requested.

3.8.2 CAG Accomplishments

Through a formal ballet and approval process, CAG was officially confirmed in July 2020 and 5 members from China, France, Germany, Philippines, and Spain have been approved. The ToR for CAG determine that the SC 27 Chair is the

Convenor of CAG. ISO/CS considered this to be not sufficient and requested a separate ballot on the CAG Convenorship, which is still ongoing (July 2020). Therefore CAG is not fully established, yet. However, CAG met three times in 2020 informally with the following topics:

- Change the spring meeting planned for St. Petersburg to a virtual meeting on March 10, 2020
- Change the autumn meeting planned for Warsaw to a virtual meeting including a virtual plenary on May 26, 2020

Discuss SC 27 guidance for proceeding a document to the next stage according to the ISO Directives

3.8.3 CAG Risks, Opportunities and Issues

Taking into account the need for more asynchronous work and more virtual meetings in the future, there will be a stronger virtualization of decision processes in all committees including SC 27. A platform like CAG can give advice to the Chair and the Committee Manager quickly and on short notice and is able to speed up decisions while increasing their quality.

3.9 Advisory Group on Strategy (AG-S)

The Scope of AG-S supports SC 27 Management on strategy with respect to upcoming technologies by

- identifying gaps in the portfolio of SC 27 standards and projects to ensure market needs are being adequately addressed,
- monitoring upcoming technologies with respect to their potential relevance of the SC 27 scope,
- reviewing issues arising from overlapping or conflicting scopes, activities, and projects as well as disagreement on project assignments between Working Groups and beyond, including Committees outside SC 27.

3.9.1 AG-S Deliverables

The AG-S does not perform any standards development work itself and only produces recommendations to SC 27 Management

3.9.2 AG-S Accomplishments

Through a formal ballet and approval process, AG-S was officially established in July 2020 and 5 members are nominated from China, Philippines, South Africa, Sweden and Switzerland.

3.9.3 AG-S Risks, Opportunities and Issues

New technology domains are expanding, and the importance and necessity of cybersecurity is unquestionable. Therefore, the need for international standards in the field of cybersecurity is expected to be increase greatly.

As a newly established group, the group should encourage the participation of experts across all fields in the near future and continue this as an ongoing effort.

3.10 Advisory Group on Operations (AG-O)

The SC 27 Advisory Group on Operations (AG-O) supports SC 27 Management on organizational issues, including aligning and coordinating WG roadmaps and the overall SC 27 roadmap, supporting handling of SC27 liaisons and common topics with other Committees, and maintaining SC 27 Standing Documents. It was created following the 2019 SC 27 Heads of Delegation meeting in Pairs in October 2019 and is composed of the SC 27 management team members, up to 15 representatives of P-Member National Bodies plus a Convenor and a Convenor Support. AG-O 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 AG-O members.

3.10.1 AG-O Accomplishments

Since 2020, the COVID-19 pandemic has brought challenges to the global conference organization, when most meetings have become virtual meetings. AG-O is actively meeting these challenges under the guidance of SC 27, and is developing the formulation of SC 27 Guidelines for Virtual Meetings. The guidelines involve virtual meeting roles and responsibilities, secure use of conference tools, timelines for meeting arrangements and principles for meeting schedules to ensure efficiency and international fairness.

In addition, in order to maintain the applicability and consistency of the SC 27 meeting guidelines, AG-O has a representative in the JTC 1 Advisory Group 17 (AG 17) on SD 19 Meetings.

3.10.2 AG-O Deliverables

AG-O has completed the draft of SC 27 Guidelines for Virtual Meetings (to be published in Q3 2020), which provides guidelines and recommendations for meeting officers, editors, and participants of the SC 27 virtual plenary and any virtual working/advisory group meetings to maximize efficiency and productivity.

3.10.3 AG-O Risks, Opportunities and Issues

Given the circumstances that virtual and mixed meeting may become the norm for a long time to come, AG-O will address guidelines for mixed mode meetings in the future.

With the adoption of the new technology platform and process requirements, AG-O will also review the current SC 27 Standing Documents and optimize related working recommendations for SC 27.

3.11 Advisory Group on Concepts and Terminology (AG-CT)

The SC 27 Advisory Group on Concepts and Terminology (AG-CT) is a new internal administrative function created to address issues with concepts and terminology across Working Groups (WGs), especially where they can affect directly or indirectly multiple WGs.

It was created following the 2019 SC 27 Heads of Delegation meeting in Paris and is composed of ten members, two from each SC27 WG including the Convenor and Convenor Support. The AG-CT 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 and its WGs. Any recommendations or organizational decisions that the AG-CT conveys to the SC 27 and its WGs shall reflect a consensus among AG-CT members. AG-CT is not empowered to make decisions on behalf of the SC 27 Plenary or WGs, except if delegation of authority is provided by the SC 27 Plenary.

3.11.1 AG-CT Deliverables

The AG-CT functions in a purely advisory capacity to SC 27 WG Management, project editors and rapporteurs. It will identify, define and prioritise terminology issues and develop approaches and methodologies to input into resolutions processes and advice. The AG-CT will monitor and report on progress but will not carry out standards development work itself.

3.11.2 AG-CT **Accomplishments**

The AG-CT produced and distributed an analysis of terms used within SC27 and the degrees to which these were inconsistent within and between WGs. The analysis provides a foundation for determining further work at both WG and SC27 level.

3.11.3 AG-CT Risks, Opportunities and Issues

Following its first report to SC 27 in Paris the Convenor and Convenor Support have been awaiting responses from WG Convenors as to their nominated representatives on the Advisory Group. Substantive work cannot begin until the team has been established.

AG-CT management has also been investigating a possible liaison with a terminology project being proposed by JTC1.

3.12 Advisory Group on Trustworthiness (AG-TW)

This advisory group has the following terms of reference:

- Provide for an environment where SC 27 members can discuss trustworthiness from a security viewpoint;
- Act as a single channel from which inputs can be made to the JTC 1 WG 13 on Trustworthiness;
- Follow the terms of reference of the ISO/IEC JTC 1 WG 13 on Trustworthiness as it is related to SC 27;
- Discuss and get consensus on contributions to be made from SC 27 to the JTC 1 WG 13.

Membership is open to all experts from all SC 27 working groups

***3.12.1 AG-TW* Accomplishments**

AG-TW is successfully participating in ISO/IEC JTC 1/WG 13.

3.12.2 AG-TW Deliverables

AG-TW provides feedback on projects directly to ISO/IEC JTC 1/WG 13. These currently are:

- Trustworthiness heatmap
- Trustworthiness vocabulary
- Trustworthiness reference architecture
- ISO/IEC 24462, Ontology for ICT Trustworthiness Assessment

3.12.3 AG-TW Risks, Opportunities and Issues

The turn-around time in ISO/IEC JTC 1/WG 13 to request and process comments is very short. This makes it difficult for AG-TW to collect comments and dispose of them in time for the WG 13 due dates.

JTC 1/SC 27 Update
Information security, cybersecurity and privacy protection

Andreas Wolf

November 2020

Highlights

- The virtual meeting in April went well: SC 27 has demonstrated that virtual meetings of large committees are possible.
- Creation of new Advisory Groups supporting better and faster processes: CAG, AG Operations, AG Strategy, AG Concepts & Terminology
- Constantly increasing attraction to the participating experts and their National Bodies: >> 1500 registered experts
- 85 Standards currently under development, 7 published in the first 6 months of 2020

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 continuously improve the visibility of SC 27 products in other standardization entities, in particular in IEC,
- Make use of the new AGs
  - Faster responses to requests from liaising organizations and
  - Improved awareness within SC 27 on relevant new technological and societal trends, and
  - Get as close as possible to the “optimal” virtual meeting
- To develop continuously and in time high quality standards according to the market needs.

ISO JTC1 IEC

INFORMATION TECHNOLOGY STANDARDS