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

JTC 1/SC 27 Business Plan 2022

Document type	Related content	Document date	Expected action
Project / Other	Meeting: Tokyo (Japan) 14 Nov 2022	2022-09-27	**COMMENT/REPLY** by 2022-10-17

Description

This document is circulated for review and consideration at the November 2022 JTC 1 Plenary.

ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection"
Secretariat: **DIN**
Committee manager: **Mahmoud Sobhi Mr**

SC 27 Business Plan 2022

Document type	Related content	Document date	Expected action
General document / Other		2022-03-22	**INFO**

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

Business Plan

Period covered: April 2022 – April 2023

1.0 Executive summary

SC 27 is an internationally recognized center of expertise serving the needs of many business sectors and 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 215 publications until December 2021, among them with ISO/IEC 27001 one of the three most popular standards within ISO, and 75 standards currently under development.

Committee membership has increased from 18 participating members in 1990 to 49 participating members (plus 32 observing members) in 2021, covering a vast area of the globe. Ten of the SC 27 members come from Africa, 14 from America, 23 from Asia Pacific, and 34 from Europe.

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.

SC 27 contributes with 23 standards to the following Sustainable Development Goals (SDG) of the United Nations:

- SDG 3 Good health and well-being
- SDG 8 Decent work and economic growth
- SDG 9 Industry, innovation and infrastructure
- SDG 10 Reduced inequalities
- SDG 11 Sustainable cities and communities
- SDG 12 Responsible consumption and production
- SDG 16 Peace, justice and strong institutions

For SC 27, gender and geographical balance is an important goal. As of December 2021, ISO Global Directory lists 1905 experts as committee members, officers or liaison representatives for SC 27 including working groups (duplicates removed). 23% of these experts are female, 77% male. 3% of the SC 27 experts come from Africa,

21% from America, 36% from Asia Pacific and 40% from Europe.

One expert from Africa, four experts from America, seven from Asia Pacific, and eleven from Europe work in SC 27 officer positions. Four out of the 23 SC 27 officers are female. Five experts from Africa, 40 from America, 92 from Asia Pacific, and 84 from Europe currently work in SC 27 editor positions. 52 out of the 221 SC 27 editors and co-editors are female.

2.0 Chairman's Remarks

This business plan has been prepared in accordance with a JTC 1 plenary resolution.

2.1 Market Requirements, Innovation

The current era of information revolution, rapid development of Internet and digital technologies has brought substantial changes in many areas, from our daily life to the processes and methods of industrial production. With this transition, standardized security techniques are becoming mandatory requirements across almost every 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 center of excellence on information security, cybersecurity and privacy protection has been at the forefront of the related standardization for 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 in recent years, so have both the membership of SC 27 and its program of work.

2.2 Communications and Outreach

SC 27 is engaged in many communication and outreach activities, managed by AG 7 and its convenor (see 3.14 for full details). The activities of AG 7 have greatly expanded the promotional activities of SC 27. The members of AG 7 are planning and managing the next generation of communication and outreach activities in SC 27.

The past twelve months have introduced new challenges and opportunities to give a greater outreach to SC 27 and its work. This has included engagement in several global issues where standardization is of a benefit to the wider stakeholder community, for example, standards in developing countries, and addressing the changing mix of cybersecurity risks that have followed from shifts in working patterns, due to COVID-19 lockdowns and work-from-home mandates. These communication and outreach activities aim to inform and encourage increased participation of experts in the work of SC 27, raise awareness of the value and benefits of SC 27 standards and increase their use and application, and to engage with communications channels, conferences and business workshops, social media, to share news and information on SC 27 accomplishments and new deliverables.

AG 7 has now launched the SC 27 Journal as an additional promotional activity: Issue 1 was released in March 2021 and Issue 2 in August 2021. The aim is to publish 2-3

issues per year. Each issue contains articles from SC 27 experts that explain the use and application of SC 27 standards. SC 27 officers and experts had the opportunity to promote the SC 27 work through various workshops, seminars and conferences.

2.3 SC 27 Conformity Assessment Protocol

SC 27 has had a number of projects involving aspects of conformity assessment (e.g. ISO/IEC 27006) for many years. Over the last two years this has increased to the extent that SC 27 has now published a protocol for coordinating advice and engagement with CASCO/CAB. This is to ensure that the correct approach is taken, in line with CASCO/CAB policy, regarding all projects involved with conformity assessment. This Protocol is implemented through a dedicated SC 27 liaison contact with CASCO/CAB. In addition,

- A team of SC 27 experts are involved as members of TMB/JTCG on all aspects of MSS policy and
- At the accreditation/certification level (which is outside of ISOs remit).

SC 27 engages with IAF using this Protocol and its external liaison channel, to help in the development of MD (IAF mandatory documents).

2.4 Accomplishments

2.4.1 Publications

Since October 2020, 37 International Standards, Technical Specifications, Technical Reports and Amendments have been published. For details see the respective WG related sections in chapter 3.

2.4.2 Resources

In 2020 and 2021, SC 27 met only in virtual mode, due to the restrictions caused by the COVID-19 pandemic. Starting in April 2020, the virtual meetings went well: SC 27 has continuously demonstrated that virtual meetings of large committees are possible. The pandemic continues. SC 27 has scheduled the two 2022 plenaries to be virtual as well, and plans to have one larger WG meeting in hybrid mode in October 2022.

Starting in 2021, SC 27 changed its meeting mode from one to two plenaries per year. In 2020 and 2021, SC 27 plenaries were conducted 18/19 September 2020, 16 April 2021, and 29 October 2021. The 2022 plenaries will take place 11/12 April 2022 and 12/13 October 2022. Since October 2020, the five SC 27 working groups held synchronized meetings before the plenary sessions. Additional synchronized meetings took place 20-24 April 2020. Furthermore, the SC 27 WGs met between the synchronized meeting events whenever it was necessary to progress their projects.

Overall, while acknowledging that there are some areas of concern, the level of engagement and expertise prove to be generally sufficient to meet the many challenges SC 27 is facing. For selected projects, SC 27 volunteers are complemented by contributors from appropriate SC 27 liaison organizations.

For continuous 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; and to make optimal use of the relevant processes and tools available, SC 27 has established the following SC 27 Advisory Groups:

- CAG: Chairman‘s Advisory Group
- AG 1/MAG: Management Advisory Group
- AG 2: Advisory Group on Trustworthiness
- AG 3: Advisory Group on Concepts and Terminology
- AG 5/AG-S: Advisory Group on Strategy
- AG 6/AG-O: Advisory Group on Operations
- AG 7/COMOG: Advisory Group on Communications and Outreach

The Advisory Group on Data Security (AG 4) was disbanded.

2.5 Competition and Cooperation (including consortia)

SC 27 benefits from collaboration with an extremely large number of productive and valuable internal and external liaisons with many committees and organizations. A complete list is available at https://www.iso.org/committee/45306.html, click at Liaisons. Selected aspects related to SC 27 liaisons are highlighted below.

2.5.1 JTC 1/SC 37 Biometrics

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 JTC 1/SC 42 Artificial Intelligence

SC 42 is responsible for standardization in the area of Artificial Intelligence and serves as the focus and proponent for JTC 1's standardization program on that topic. Furthermore, SC 42 provides guidance to JTC 1, IEC, and ISO committees developing AI applications. Many AI related standards contain IT security and privacy related components and therefore require close cooperation between SC 27 and SC 42.

2.5.3 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:

- Information security management guidelines for telecommunications (Recommendation ITU -T X.1051 and ISO/IEC 27011:2016)
- Governance of information security (Recommendation ITU-T X.1054 and ISO/IEC 27014:2020)
- Telebiometric authentication framework using biometric hardware security module (Draft Recommendation ITU-T X.1085 (bhsm) and ISO/IEC 17922:2017)
- Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Recommendation ITU-T X.1631 (cc-control) and ISO/IEC

27017:2015)
- Code of practice for the protection of personally identifiable information (Draft Recommendation ITU-T 1058 (X.gpim) and ISO/IEC 29151:2017)

2.5.4 The Common Criteria Development Board (CCDB)

The CCDB and SC 27/WG 3 have had a long-standing technical liaison on projects related to IT Security Evaluation Criteria. Thus, working group 3 has been working in close co-operation with the CCDB on the current revision process of ISO/IEC 15408 and ISO/IEC 18045. This close cooperation has allowed these two standards to be revised taking into consideration the contributions from the CCRA stakeholders, certification bodies using the referred standards.

The path of cooperation is extended to the roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045, which aims at setting up priorities for the future revision of the aforementioned standards. A significant number of SC 27/WG 3 projects complement the application of ISO/IEC 15408, such as ISO/IEC TS 22216, Introductory guidance on evaluation for IT security, ISO/IEC IS 23532, Requirements for the competence of IT security testing and evaluation laboratories, and ISO/IEC 19896, Competence requirements for information security testers and evaluators.

Several new work items of SC27/WG3 are of interest to the CCDB, namely:

- Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045
- Cybersecurity assurance complex systems based on of systems and system of systems (SoS) based on ISO/IEC 15408
- Requirements for the competence of ITC products cybersecurity conformity assessment body personnel – Knowledge, skills and effectiveness for ISO/IEC 15408 and ISO/IEC 19790 validators

This extended coverage increases the collaboration with the CCDB.

2.5.5 ISO/TC 292 Security and resilience

ISO/TC 292 has a broad scope covering "Standardization in the field of security and resilience of society". SC 27 has established a close cooperation with TC 292 on topics of common interest. SC 27/WG 1 and WG 4 have a particular interest in the following TC 292 projects:

- The ISO 22300 family of standards including;
    - New edition of ISO 22300, Security and resilience – Vocabulary
    - ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements
    - ISO 22313:2020, Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301
    - ISO 22316:2017, Security and resilience – Organizational resilience – Principles and attributes
    - ISO/TS 22317, Security and resilience – Business continuity management

systems – Guidelines for business impact analysis
    - ISO/TS 22318, Security and resilience – Business continuity management systems – Guidelines for supply chain continuity
    - ISO 22320:2018, Security and resilience – Emergency management – Guidelines for incident management
    - ISO/TS 22332, Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures
    - ISO 22385, Security and resilience – Authenticity, integrity and trust for products and documents
- The ISO 28000 family of standards including;
    - Revision of ISO 28000 – Specification for security management systems for the supply chain
    - ISO 28001:2007, Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
    - ISO 28002:2011, Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
- ISO 31050 Risk management – Guidance for managing emerging risks to enhance resilience (joint work between TC 292 and TC 262)

2.5.6 ISO/TC 232 Education and learning services

The scope and work of ISO/TC 232 (education and learning services), in particular ISO 21001:2018, Educational organizations – Management systems for educational organizations – Requirements with guidance for use, is of interest to SC 27/WG 1 and its work on cyber education and training. SC 27 has established liaison with TC 232 to explore areas of common interest.

2.5.7 ISO/TC 309 Governance of organizations

The scope and work of ISO/TC 309 (governance of organizations), in particular ISO 37301 Compliance management systems - Requirements with guidance for use, is of interest to SC 27/WG 1, especially related to its work on information security governance ISO/IEC 27014 and its information security management system standard ISO/IEC 27001.

2.5.8 ISO/TC 307 Blockchain and distributed ledger technologies

ISO/TC 307 was created in 2016 and has the scope to standardize blockchain and distributed ledger technologies. It intends to cover not only the technologies used to implement and support blockchain and distributed ledgers, but also the generic requirements for their application in sector specific environments.

Many of the fundamental technologies used by blockchain and distributed ledgers make use of 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 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 through JWG 4. The collaboration between SC 27 and ISO/TC 307 has benefitted from the existence of this JWG. Areas of common interest for 2022 are identity, privacy and security.

2.5.9 IEC Advisory committee on information security and data privacy (ACSEC)

ACSEC deals with information security and data privacy matters which are not specific to any one single IEC technical committee. It coordinates activities related to information security and data privacy, and provides advice to IEC/SMB on those subjects. ACSEC provides guidance to TC/SCs for implementation of information security and data privacy in a general perspective and for specific sectors. ACSEC also provides a venue for exchanging information between IEC and other standards developing organizations relevant to ACSEC's scope. ACSEC follows closely both research activities and trends in academia. By participating in ACSEC, SC 27 promotes the application of SC 27 standards in IEC committees, and receives updates on standardization needs with respect to IT security from the IEC world.

2.5.10 IEC/TC 65 Industrial process measurement, control and automation

SC27 has had a long and mutually very beneficial liaison relationship with IEC/TC 65 in the field of cybersecurity standardization, particularly in security management and the specification of security functionality. SC27 members have participated in the development of the IEC 62443 series of standards for security of industrial automation and control systems and vice versa. IEC/TC 65 has recently been given responsibility by the IEC Standardization Management Board (SMB) for the horizontal function of cybersecurity within all Operational Technologies, and therefore this liaison relationship will become even more important in maintaining consistency between IT and OT cybersecurity standardization activities.

3.0 SC 27 program of work

3.1 WG 1 – Information security management systems

SC 27/WG 1 develops, manages and maintains the ISO/IEC 27000 family of 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 the SC 27 public website at www.din.de/go/jtc1sc27.

3.1.1 WG 1 accomplishments

Since October 2020, WG 1 has completed work on the following documents:

- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls
- ISO/IEC 27013:2021, Information security, cybersecurity and privacy protection – Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27021:2017/Amd 1:2021, Information technology – Security techniques – Competence requirements for information security management systems professionals – Amendment 1: Addition of ISO/IEC 27001:2013 clauses or sub-clauses to competence requirements
- ISO/IEC TS 27022:2021, Information technology – Guidance on information security management system processes
- ISO/IEC TS 27100:2020, Information technology – Cybersecurity – Overview and concepts
- ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

3.1.2 WG 1 deliverables

With the publication of the 3rd edition of ISO/IEC 27002, WG 1 has launched a phased revision programme for all those standards that will need to be updated to be aligned with this third edition. This includes: ISO/IEC 27001, 27003, 27008, 27009, 27010, 27011, 27017, 27019 and ISO/IEC 27103. WG 1 is also progressing the development of a number of documents including (current status in parenthesis):

- ISO/IEC DIS 27005, Information security, cybersecurity and privacy protection – Guidance on managing information security risks and opportunities (revision)
- ISO/IEC CD 27006-1, Requirements for bodies providing audit and certification of information security management systems – Part 1: General
- PWI 27028 guidelines for ISO/IEC 27002 attributes
- PWI 27029 ISO/IEC 27002 and ISO and IEC standards
- PWI 27109 cyber education and training

Other deliverables include the Standing Documents SD 7 (Use of ISO/IEC family of standards in Governmental/Regulatory requirements), which is being converted into a TR ISO/IEC 27024, SD 2 (Guidance and terminology processes) and a PWI on cyber education and training. Finally, WG 1 has embarked on preparatory work for sector specific certification requirements as an extension to ISO/IEC 27006.

3.1.3 WG 1 strategies/risks/opportunities/lessons learned

ISO/IEC 27001 family – a global phenomenon: The established market global position of ISO/IEC 27001 and ISO/IEC 27002 as bestselling ISO/IEC standards in information security management is an outstanding achievement. As well as these standards being classified by ISO as very high profile, a distinction reserved for very few standards, ISO/IEC 27001 is also ranked fourth in the ISO survey of Management System Standards (MSSs). These standards provide a common international language

that facilitates many opportunities for growth and harmonization across all market sectors.

Risks: The universal nature of ISO/IEC 27001 for all information security and cybersecurity management requirements is designed to avoid the non-proliferation of MSS. In order that remains the case JTC 1 and SC 27 should protect ISO/IEC 27001 against the risk of the unnecessary proliferation of additional MSS (e.g. sector-specific MSS) by curbing their development and only endorsing disciple-specific MSS: security (ISO/IEC 27001) and privacy (ISO/IEC 27701).

Strategic developments: WG 1 has other strategic developments that address the diverse and continual increase in cyber risks and to support cyberspace governance such as the successful ISO/IEC 27005, and ISO/IEC 27014. The work of WG 1 has generated a set of world class horizontal standards with significant outreach for customer and societal demands and requirements, and with benefits for sector/application specific markets. 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.

Strategic engagements: WG 1 continues to play a pro-active role in ISO/TMB/JTCG Joint Technical Coordination Group on MSS in shaping the future of MSS. Also, WG 1 actively liaises with IAF (International Accreditation Forum) and engages with CASCO/CAB concerning aspects of conformity assessments through the SC 27 Protocol (see 2.3), in particular regarding the accreditation, auditing and certification standards (e.g. ISO/IEC 27006-1, and ISO/IEC 27007). WG 1 also engages with other committees dealing with MSS such as ISO/TC 292 (security and resilience), ISO/PC 302 (assessment), TC 309 (governance), TC232 (education) and ISO/TC 262 (risk management), and with IEC committees TC 45, TC 57 and TC 65 on cyber and sector-specific aspects of the WG1 ISMS projects. WG 1 has a close working relationship with ITU-T SG 17 through which several common-text standards have been produced: ISO/IEC 27011, ISO/IEC 27014 and ISO/IEC 27017.

International ISO/IEC 27001 day: WG 1 has launched the International ISO/IEC 27001 Day on 27 January 2022 to celebrate this successful standard and its high profile position in the global marketplace.

3.2 WG 2 – Cryptography and security mechanisms

WG 2 deals with cryptography and security mechanisms. WG 2 has the task to identify the need and requirements for these techniques and mechanisms in IT systems and applications and to develop 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 2020, WG 2 has completed work on the following documents:

- ISO/IEC 9797-2:2021-06, Information security – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function
- ISO/IEC 10118-1:2016/AMD1:2021-03, Information security – Hash-functions – Part 1: General – Amendment 1
- ISO/IEC 11770-3:2021-10, Information security – Key management –Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 11770-7:2021-07, Information security – Key management –Part 7: Cross-domain password-based authenticated key exchange
- ISO/IEC 18014-2:2021-09, Information security – Time-stamping services – Part 2: Mechanisms producing independent tokens
- ISO/IEC 18033-1:2021-09, Information security – Encryption algorithms – Part 1: General
- ISO/IEC 18033-3:2010/AMD1:2021-06, Information security – Encryption algorithms – Part 3: Block ciphers – Amendment 1
- ISO/IEC 23264-1:2021-03, Information security – Redaction of authentic data – Part 1: General

3.2.2 WG 2 deliverables

WG 2 is progressing the development of a number of documents including (current status in parenthesis):

- ISO/IEC 4922-1 (DIS), Information security – Secure multiparty computation – Part 1: General
- ISO/IEC 4922-2 (CD), Information security – Secure multiparty computation – Part 2: Mechanisms based on secret sharing
- ISO/IEC 9797-1/AMD1 (CDAM), Information security – Message authentication codes (MACs) – Part 1: Mechanisms using a block cipher – Amendment 1
- ISO/IEC 15946-5 (FDIS), Information security – Cryptographic techniques based on elliptic curve – Part 5: Elliptic curve generation (revision)
- ISO/IEC 18033-7 (FDIS), Information security – Encryption algorithms – Part 7: Tweakable block ciphers
- ISO/IEC 20008-2/AMD2 (DAM), Information security – Anonymous digital signatures – Part 2: Mechanisms using a group public key – Amendment 2
- ISO/IEC 20009-3 (FDIS), Information security – Anonymous entity authentication – Part 3: Mechanisms based on blind signatures
- ISO/IEC 23264-2 (CD), Information security – Redaction of authentic data – Part 2: Redactable signature schemes based on asymmetric mechanisms
- ISO/IEC 29192-8 (FDIS), Information security – Lightweight cryptography – Part 8: Authenticated encryption

WG 2 is currently developing new standards, including:

- ISO/IEC 14888-4, Information security – Digital signatures with appendix – Part

4: Stateful hash-based mechanisms
- ISO/IEC 18033-8, Information security – Encryption algorithms – Part 8: Fully homomorphic encryption

WG 2 is also studying a few potential new topics as Preliminary Work Items, including:

- Modes of operation for tweakable block ciphers
- Inclusion of arithmetization-friendly cryptographic algorithms in ISO/IEC standards
- Amendment of Identity-Based Authenticated Key Exchange
- Consideration of the Security Model for Mechanism 7a in ISO/IEC 9798-6

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 areas of interest include:

- 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

Since October 2020, WG 3 has completed work on the following documents:

- ISO/IEC TS 23532-1:2021, Information security, cybersecurity and privacy protection – Requirements for the competence of IT security testing and evaluation laboratories – Part 1: Evaluation for ISO/IEC 15408
- ISO/IEC TS 23532-2:2021, Information security, cybersecurity and privacy protection – Requirements for the competence of IT security testing and evaluation laboratories – Part 2: Testing for ISO/IEC 19790
- ISO/IEC 20897-1:2020, Information security, cybersecurity and privacy protection – Physically unclonable functions – Part 1: Security requirements

3.3.2 WG 3 deliverables

WG 3 is progressing the development of a number of documents, including (current status in parenthesis):

- ISO/IEC 15408 (FDIS), Information security, cybersecurity and privacy protection – Evaluation criteria for IT security
    - Part 1: Introduction and general model (revision)
    - 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 (FDIS), Information security, cybersecurity and privacy protection – Methodology for IT security evaluation (revision)
- ISO/IEC 20897-2 (DIS), Information security, cybersecurity and privacy protection – Physically unclonable functions – Part 2: Test and evaluation methods
- ISO/IEC TR 22216 (DTR), Information security, cybersecurity and privacy protection – New concepts and changes in ISO/IEC 15408:2021 and ISO/IEC 18045:2021
- ISO/IEC 23837-1 (CD), Information technology security techniques – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements
- ISO/IEC 23837-2 (CD), Information technology security techniques – Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods
- ISO/IEC 24485 (DTR), Information technology – Security techniques – Security properties, test and evaluation guidance for white box cryptography
- ISO/IEC 29128-1 (DIS), Information security, cybersecurity and privacy protection – Verification of cryptographic protocols – Part 1: Framework
- ISO/IEC 5891 (DTR), A general framework for runtime hardware security assessment
- ISO/IEC 5895 (DTR), Multi-party coordinated vulnerability disclosure and handling

3.3.3 WG 3 strategies/risks/opportunities/lessons learned

WG 3 is finishing 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, as it is the first time that WG 3 has lead the maintenance and evolution of the referred standards, working as always in close coordination with the CCDB. This revision is scheduled to be completed in 2022, aiming to provide an improved standard able to cope with the new demands of cybersecurity evaluation and certification.

The candidate EUCC certification scheme, a proposal to implement a European-wide product certification scheme, makes extensive use of WG3 standards. This is a significant development that will drive further work within WG 3.

As the WG 3 products gain such popularity, coverage of assurance concepts and cybersecurity evaluation criteria and methodology on new challenging areas is the topic of several preliminary work items, addressing the cybersecurity assurance of complex systems, security evaluation of biometrics or requirements for the competence of IT security conformance assessment body personnel.

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 like readiness, continuity, incident and event management, investigation
- Information life cycle like creation, processing, storage, transmission and disposal
- Organizational processes like design, acquisition, development and supply
- Security aspects of Trusted services like in the provision, operation and management of these services
- Cloud, internet and cyber security related technologies and architectures like network, virtualization, storage
- Digital environments, such as cloud computing, cyber, Internet, and other organizations

3.4.1 WG 4 accomplishments

Since October 2020, WG 4 has completed work on the following documents:

- ISO/IEC 27036-1:2021, Cybersecurity – Supplier relationships – Part 1: Overview and concepts
- ISO/IEC 27050-4:2021, Information technology – Electronic discovery – Part 4: Technical readiness
- ISO/IEC 27070:2021, Information technology – Security techniques – Requirements for establishing virtualized roots of trust

3.4.2 WG 4 deliverables

WG 4 is progressing the development of several documents, including (current status in parenthesis):

- ISO/IEC 27036-2 (DIS), Cybersecurity – Supplier relationships – Part 2: Requirements
- ISO/IEC 27099 (DIS), Information technology – Public key infrastructure – Practices and policy framework
- ISO/IEC 27400 (DIS), Cybersecurity – IoT security and privacy –Guidelines

3.4.3 WG 4 strategies/risks/opportunities/lessons learned

The need for International Standards in big data and AI, 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 (JTC 1/SC 7 and JTC 1/SC 42), and Internet of Things (JTC 1/SC 25 and 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 example 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

Since October 2020, WG 5 has completed work on the following documents:

- ISO/IEC TS 27006-2:2021, Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy Information Management Systems (this activity was started as 27558)
- ISO/IEC TS 27570:2021, Information technology – Security techniques – Privacy guidelines for smart cities
- ISO/IEC 27551:2021, Information security, cybersecurity and privacy protection – Requirements for attribute-based unlinkable entity authentication
- ISO/IEC 27555:2021, Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion

3.5.2 WG 5 deliverables

WG 5 is progressing the development of a number of documents including (current status in parenthesis):

- ISO/IEC 24745 (under publication) Information security, cybersecurity and privacy protection – Biometric information protection
- ISO/IEC 24760-2 (CD) Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
- ISO/IEC 24760-3:2016 Amd1 (CD) Information technology – Security techniques – A framework for identity management – Part 3: Practice
- ISO/IEC 27006-2:2021 (WD) Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy Information Management Systems
- ISO/IEC 27553-1 (DIS) Information security, cybersecurity and privacy protection – Security and Privacy requirements for authentication using biometrics on mobile devices – Part 1: Local modes
- ISO/IEC 27553-2 (PWI) Information security, cybersecurity and privacy protection – Security and Privacy requirements for authentication using biometrics on mobile devices – Part 2: Remote modes
- ISO/IEC 27554 (CD) Application of ISO 31000 for assessment of identity - related risk
- ISO/IEC 27556 (DIS) Information security, cybersecurity and privacy protection

– User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences
- ISO/IEC 27557 (DIS) Information technology – Information security, cybersecurity and privacy protection – Organizational privacy risk management
- ISO/IEC 27559 (DIS) Privacy enhancing data de-identification framework
- ISO/IEC TS 27560 (WD) Privacy technologies – Consent record information structure
- ISO/IEC TS 27561 (WD) Information technology – Security techniques – Privacy operationalisation model and method for engineering (POMME)
- ISO/IEC 27562 (WD) Privacy guidelines for fintech services
- ISO/IEC TR 27563 (DTR) Impact of security and privacy in artificial intelligence
- ISO/IEC 27564 (PWI) Privacy models
- ISO/IEC 27565 (NP) Guidelines on privacy preservation based on zero knowledge proofs
- ISO/IEC 29134:2017/Amd 1 (CD) Information technology – Security techniques – Guidelines for privacy impact assessment – Amendment 1
- ISO/IEC 29146:2016/Amd 1 (DAM) Information technology – Security techniques – A framework for access management – Amendment 1

3.5.3 WG 5 strategies/risks/opportunities/lessons learned

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 applied. Moreover, the group is attracting more volunteers. The trend is an opportunity and a challenge, as the group is growing and the privacy work elsewhere is also intensified. Therefore, WG 5 is continuing to maintain many liaisons. In particular liaisons with research projects continue to be very successful: relevant innovative content was contributed and more volunteers participated in WG5.

The ISO/COPOLCO initiated project ISO 31700, Privacy by design for consumer goods and services, has been assigned by ISO/TMB to ISO/PC 317. WG 5 contributes to this project in close collaboration with PC 317, including holding joint or back-to-back meetings.

The WG 5 experience with virtual only meetings showed that virtual meetings can be arranged easily compared to physical ones. However, their effectiveness is sometimes lower, as they don’t enable the full spectrum of interaction the standardization process needs, especially in a very interdisciplinary field in highly contested national and international regulatory environment and for innovative approaches. Therefore WG 5 is very happy to have received an invitation by the Luxembourg National Body ILNAS to trial a hybrid meeting, knowing that this will require major infrastructural effort for the host. ILNAS has offered to host the hybrid WG 5 meeting in the week of September 26-30, 2022. The organization process is underway.

3.6 Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices

The security of connected vehicle was of interest to both ISO/IEC JTC1/SC 27 and ISO/TC 22/SC 32. In order to fully leverage the expertise of the two parents committees, JWG 6 has been established in Oct 2021 between ISO/IEC JTC1/SC 27 and ISO/TC 22/SC 32. The scope of JWG 6 covers aspects related to security requirements and evaluation activities for connected vehicle devices. This JWG is under the administrative responsibility of ISO/IEC JTC 1/SC 27.

3.6.1 JWG 6 deliverables

JWG 6 is progressing the development of the following document:

- NWIP 5888, Information security, cybersecurity and privacy protection – Security requirements and evaluation activities for connected vehicle devices

3.6.2 JWG 6 strategies/risks/opportunities/lessons learned

JWG 6 was created to leverage different expertise and competences from the two parents committees. The security evaluation methodology and system of ISO/IEC JTC1/SC 27 can be used in developing international standard of connected vehicle devices. In JWG 6, the related international standards and document will be developed and fully discussed to meet the need of International Standards to avoiding duplications and possible inconstancies. With the remit of considering security from different sides, it will be challenging to manage this JWG to meet various industry needs and security requirements. In addition, security is a horizontal issue in different fields, the operation of a JWG could provide experience for future work of ISO/IEC JTC1/SC 27.

3.7 ISO/TC 307-JTC 1/SC 27/JWG 4 – Security, privacy and identity for Blockchain and DLT

JWG 4 has started its activities in 2018. This JWG is under the administrative responsibility of ISO/TC 307. The 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.

3.7.1 JWG 4 accomplishments

Since Jan 2020, JWG 4 has completed work on the following document:

- ISO/TR 23244 Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations

3.7.2 JWG 4 deliverables

JWG 4 is progressing the development of the following documents (current status in parenthesis):

- ISO/TR 23249 (under publication), Overview of existing DLT systems for identity management

- ISO/WD TR 23644 (DTR) Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management

3.7.3 JWG 4 strategies/risks/opportunities/lessons learned

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 for the production of specialized standards in the intersection of the two parent committees while avoiding duplications and possible inconstancies. 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 program 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.

3.8 Chair Advisory Group (CAG)

3.8.1 CAG Accomplishments

CAG consists of the SC 27 chair, chair support and committee manager, of the convenors of the five working groups, and seven NB members from Argentina, China, France, Germany, India, Philippines, and Spain. Since October 2020, CAG met five times with the following agenda items, supported by some consultations:

- Location, timing and duration of the next and future meetings(s)
- Announcement of meeting series in the ISO meeting platform, meeting information template
- MAG composition and membership
- Projects on hold due to CASCO/CAB concerns, future consideration of CASCO/CAB related aspects
- AG 5 and AG 6 status and updates
- Expert/NB questionnaire on meeting conditions

3.8.2 CAG Deliverables

CAG does not develop deliverables itself. CAG supports the SC 27 chair in leading SC 27 between the Plenaries. CAG gives 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.

3.8.3 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 AG 1 – Management Advisory Group

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 in 2017 and is composed of ten members including a convenor and convenor support officer nominated by National Bodies and representing the membership from all SC 27 working groups, with geographical balance. 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 restricted to MAG members.

3.9.1 AG 1 Accomplishments

During this period MAG presented several proposals to the SC 27 management for improvement of meeting management and working group organization in order to improve SC27 efficiency.

MAG has been also addressing the impact of virtual meetings on SC27 efficiency and has made improvement proposals to SC27 management. Many of these improvements have been adopted by the SC27 management team and are in operation. In particular desynchronization, remote preparation meetings and having two plenaries per year.

3.9.2 AG 1 Deliverables

MAG does not perform any standards development work itself and only produces recommendations or food for thought for SC 27 management.

3.9.3 AG 1 Risks, Opportunities and Issues

MAG is currently working on improvement of SC27 functioning given the major 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 and following 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. In addition, MAG is working on topics like the IPR issue and cost of standards which are now critical points as for example with Common Criteria standards (ISO/IEC 15408/18045).

3.10 AG 2 – Trustworthiness

This advisory group has the following terms of reference:

- Provide for an environment where SC 27 members can discuss trustworthiness from a security and privacy viewpoint
- Act as a single channel from which inputs can be made to JTC 1/WG 13 on Trustworthiness
- Follow the projects of the ISO/IEC JTC 1/WG 13 on Trustworthiness as it is related to SC 27
- 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 within AG 2 to be made as contributions from SC 27 to JTC 1/WG 13

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

3.10.1 AG 2 Accomplishments

AG 2 is successfully participating in ISO/IEC JTC 1/WG 13.

3.10.2 AG 2 Deliverables

AG 2 contributes directly to ISO/IEC JTC 1/WG 13 projects such as:

- JTC 1 Standing document Landscape of trustworthiness
- ISO/IEC TS 5723, Trustworthiness – Vocabulary
- ISO/IEC PWI 5957, Trustworthiness – Reference architecture
- ISO/IEC PWI 9814, Trustworthiness – Overview and concepts

3.10.3 AG 2 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 2 to collect comments and dispose of them in time for the WG 13 due dates.

3.11 AG 3 – Concepts and Terminology

The SC 27 Advisory Group on Concepts and Terminology is an SC 27 internal administrative function created to address issues with concepts and terminology across working groups, especially where they can affect directly or indirectly multiple WGs.

It was created in 2019 and is composed of the AG 3 convenor and AG 3 convenor support as well as ten members, two from each SC27 WG. The AG 3 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 3 conveys to the SC 27 and its WGs shall reflect a consensus among AG 3 members. AG 3 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 3 Accomplishments

The AG 3 produced and distributed an analysis of terms used within SC 27 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 SC 27 level.

3.11.2 AG 3 Deliverables

The AG 3 functions in a purely advisory capacity to SC 27 WG management, project editors and rapporteurs. It identifies, defines and prioritizes terminology issues and develops approaches and methodologies to input into resolutions processes and advice. The AG 3 monitors and reports on progress but does not carry out standards development work itself.

3.11.3 AG 3 Risks, Opportunities and Issues

AG 3 depends on the support from WG convenors and experts to their nominated representatives on the Advisory Group. Substantial work can only be done with an established team. AG 3 also contributes to the work of JTC 1/AG 18 on JTC 1 vocabulary, and delegates one of its members as SC 27 representative to AG 18.

3.12 AG 5 – Strategy

The Scope of AG 5 is to support the SC 27 management by providing strategic advice with respect to upcoming technologies by

- Identifying gaps in the portfolio of SC 27 standards and projects, determining where market needs are not 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

3.12.1 AG 5 Deliverables

AG 5 does not perform any standards development work itself and only produces recommendations to the SC 27 management. AG 5 is however responsible for the maintenance of two SC 27 Standing Documents, SD 17, Information Security Library, and SD 19, Risk Management Resource Library.

AG 5 has so far coordinated and drafted responses on behalf of SC 27 management to external detailed requests and completion of questionnaires, e.g., smart manufacturing.

3.12.2 AG 5 Accomplishments

AG 5 was established in July 2020 with 11 experts. Members from Belgium, China, Great Britain, India, Korea, Philippines, South Africa, Sweden, and Switzerland were approved, in addition the SC 27 management and the WG convenors are ex-officio members of AG 5.

3.12.3 AG 5 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 increase greatly. The group continues to encourage the participation of experts across all fields of JTC 1 and remains open to input and contributions from all relevant international standardization activities.

3.13 AG 6 – Operations

The SC 27 Advisory Group on Operations supports the SC 27 management on organizational issues, including aligning and coordinating WG roadmaps and the overall SC 27 roadmap, supporting handling of SC 27 liaisons and common topics with other committees, and maintaining SC 27 standing documents. It was created in 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. Currently, the 11 AG 6 NB members come from Argentina, Belgium, China, Germany, Great Britain, Korea, India, Sweden, and Switzerland. AG 6 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 6 members.

3.13.1 AG 6 Accomplishments

Since 2020, the COVID-19 pandemic has brought challenges to the global conference organization, when most meetings have become virtual meetings. AG 6 is actively meeting these challenges under the guidance of SC 27, and has developed the 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 6 is represented in the JTC 1/AG 17 on SD 19.

3.13.2 AG 6 Deliverables

AG 6 has published the SC 27 Guidelines for virtual meetings, which provide 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.

3.13.3 AG 6 Risks, Opportunities and Issues

Given the circumstances that virtual and mixed meetings may become the norm for a long time to come, AG 6 intends to develop guidelines for mixed mode meetings in the future. The SC 27 plenary assigned the maintenance of several SC 27 standing documents to AG 6. With the adoption of the new technology platform and process

requirements, AG 6 will review the current SC 27 standing documents and optimize related working recommendations for SC 27.

3.14 AG 7 – Communications and Outreach Advisory Group (COMOG)

3.14.1 AG 7 Scope and Objectives

AG 7 is responsible for all communication and outreach activities related to SC 27, its working groups and advisory groups, and its work programme. The objectives of COMOG are thus to:

- 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

AG 7 works together with ISO/CS, JTC 1/AG 01 (Communications Advisory Group) and AG 10 (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)

3.14.1 AG 7 Accomplishments and Deliverables

AG 7 delivers a range of promotional materials, publications and articles to support and communicate the work of SC 27. It also engages in external projects, workshops and conferences to raise awareness of SC 27 and its work as well provide opportunities for engagement with industry and business to cultivate and foster standardization activities and future cooperation.

Articles: A number of articles and press releases were published over the last 12 months. These include:

- https://www.iso.org/news/ref2629.html (2021-02-16) - Keeping cybersafe
- https://www.iso.org/contents/news/2021/01/Ref2613.html (2021-01-14) - Biometric security
- https://www.iso.org/news/ref2495.html (2020-12-16) - Keeping an eye on information security
- https://www.iso.org/news/ref2578.html (2020-11-05) - Getting big on data
- https://www.iso.org/news/ref2563.html (2020-10-02) - Keeping cyberspace safe for 30 years
- https://www.iec.ch/blog/cyber-security-it-and-ot-supply-chains (2021-02-03) - Cyber security for IT and OT supply chains
- https://etech.iec.ch/issue/2021-01/securing-it-and-ot-supply-chains-with-international-standards-and-conformity-assessment (2021-02-01) - Securing IT and OT supply chains with international standards and conformity assessment

SC 27 Journal: Two issues of the SC27 Journal were released in 2021 and one in 2022, with more planned for 2022:

- SC 27 Journal Issue 1 (WG 1 articles) released March 2021
- SC 27 Journal Issue 2 (WG 4 articles) released August 2021
- SC 27 Journal Issue 3 (WG 2 articles) released February 2022
- SC 27 Journal Issue 4 (WG 3 articles) and Issue 5 (WG 5 articles) in 2022

SD 11: There were two editions of SD 11, Overview of SC 27 Structure, Members and Work Programme, in 2021. There will be two further editions published in 2022.

SC 27 gender study: The development of the SC 27 Gender Study is well under way. A preliminary draft of the AG07 study is to be attached to a future edition of this report. AG07 plans to release a questionnaire for the further development and possible finalisation of the report. AG07 has been collecting data from the WGs on gender representation. The data shows good representation at the editor level, but a need to build a better gender balance at the officer and expert levels. At the expert level, improvement in the parity of membership to achieve a more balanced mix of males and females will ensure a better level of gender representation. Part of the solution will be raising awareness among SC 27 members, the community of experts, working groups and stakeholders the need to improve expert gender representation. A SC 27 gender awareness workshop may be proposed for NBs. The UN/IEC SDGs 5 and 10 are highly relevant to this study and to the greater mission of the ISO activity. In addition, SDG 3 plays an important role, not only as a general SC 27 target for future work but particularly appropriate to gender engagement in standardization work on information security, cybersecurity and privacy protection. We can add to this SDG 8, 9 and 15 as important to the expansion of gender equality across the workforce and the responsiveness to information security, cybersecurity and privacy protection standards.

SC 27 SDGs: The current listing of Sustainable Develop Goals (SGDs) linked to SC 27 projects is being updated since there are far more SC 27 projects associated with SGDs than appears on the ISO site. The 2030 UN agenda is an important schedule of commitment which SC 27 is already a part of, however, there is much more to be done within SC 27 to contribute to the 2030 sustainability plan. AG7 will be collecting information from WGs to improve our standing in the ISO list. Also, there are areas within the three pillars (economic, social and environment) of sustainable development outlined by the UN that SC 27 needs to consider within its programme of work. The work of SC 27 on information security, cybersecurity and privacy protection touches upon each of these three pillars, and its WGs have much to offer the UN programme. AG7 will be reporting on these additional considerations within the scope of SC 27 and presenting recommendations for future work engagements that could expand our commitment and SDG outreach.

Workshops, seminars, conferences: SC 27 officers and experts have continued to promote the SC 27 work through various on-line workshops, seminars and conferences throughout 2021.

3.14.2 AG 7 Risks, Opportunities and Issues

As the scope and diversity of work in SC 27 continues to grow and expand so does the work of AG 7 to communicate the accomplishments and successes of SC 27 to the global community. Many opportunities await AG 7 in the coming years as the SC 27 interface to the outside world extends to embrace new ways of communication and outreach. For example, AG 7 plans to take SC 27 into the world of social media with the development of a SC 27 hosted Web site and a SC 27 Facebook planned for 2021/2022.