ISO/IEC JTC 1/SC 27 N19988
SD18

REPLACES: N17528

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

Secretariat: DIN, Germany

DOC TYPE:	standing document
TITLE:	**SC 27 SD18 – SC 27 Structure and scope**
SOURCE:	**JTC 1/SC 27 Committee Manager**
DATE:	2019-09-25
PROJECT:	**SD18**
STATUS:	**As per Tel Aviv Resolution 27 (contained in N19900) of the 31st SC 27 Plenary meeting held in Tel Aviv, Israel, 8th – 9th April 2019 the hereby attached text of SD18 was updated. It is forwarded for review and approval by the SC 27 HoD meeting in Paris, France, 17th October 2019. It is also circulated within SC 27 for information.**
ACTION ID:	**ACT/INFO**
DUE DATE:	
DISTRIBUTION:	P, O, L Members L. Rajchel, JTC 1 Committee Manager J. Alcorta, ISO/CS (ITTF) A. Wolf, SC 27 Chair L. Lindsay, SC 27 Vice-Chair E. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors J.-P. Quémard, MAG-Convenor A. Fuchsberger, SWG-Convenor
MEDIUM:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27
NO. OF PAGES:	1 + 11

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627 [D-10772 postal] Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-4-2652; E-mail: krystyna.passia@din.de
HTTP://www.din.de/go/jtc1sc27

1 Purpose

The purpose of this SC 27 Standing Document 18 (SD18) is to provide the approved scopes of the ISO/IEC JTC 1/ SC 27 – Information technology – Security techniques and its various Working Groups (WGs) and to identify the key areas of work within these groups.

2 SC 27

2.1 Scope

Development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management system (ISMS) standards, security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure that its work reflects the needs of relevant sectors in society and the proper application of SC 27 standards and technical reports as appropriate.

3 Working Groups

3.1 WG 1 – Information Security Management Systems

WG 1 is the centre of international expertise on all standardisation matters regarding Information Security Management System (ISMS) standards. The scope of WG 1 covers the development of ISMS standards and guidelines.

This includes:

- Development and maintenance of the ISO/IEC 27000 ISMS standards family. This includes, besides ISO/IEC 27001 and ISO/IEC 27002, ISMS guidelines and supporting documentation, for example, for ISMS implementation, information security management measurements, information security risk management;
- Information security management systems requirements
- Accreditation, certification requirements and auditing standards;
- Competence requirements standards for information security management systems professionals;
- Sector specific ISMS application standards;
- Information security management governance and economics;

WG 1 collaborates with other Working Groups in SC 27, in particular with WG 4 and WG 5 on standards addressing the implementation of control objectives and controls as defined in ISO/IEC 27001 and ISO/IEC 27002.

WG 1 develops and maintains the WG 1 standing documents.

WG 1 ensures liaison and collaboration with those organisations and committees dealing with specific requirements and guidelines for ISMS.

3.2 WG 2 – Cryptography and Security Mechanisms

WG 2 provides the centre of expertise for the standardisation of ICT security techniques and mechanisms within JTC 1 with the following scope:

- Identification of the needs and requirements for ICT security techniques and mechanisms in ICT systems and applications;
- Development and maintenance of terminology, general models and standards for these techniques and mechanisms for use in security services;
- Development and maintenance of WG 2 standing documents

The ICT security techniques include:

- confidentiality;
- entity authentication;
- non-repudiation;
- key management, including random number generation and prime number generation;
- data integrity such as message authentication, hash-functions and digital signatures.

The mechanisms in general specify several options with respect to the (combination of) cryptographic techniques used, including symmetric and asymmetric cryptographic, and non-cryptographic.

WG 2 collaborates with other Working Groups in SC 27, in particular with WG 3 on evaluation aspects and WG 5 on identity management, biometrics and the protection of personal data.

WG 2 develops and maintains the WG 2 standing documents.

WG 2 ensures liaison and collaboration with those organisations and committees dealing with specific requirements related to ICT security techniques and cryptography.

3.3 WG 3 – Security Evaluation, Testing and Specification

WG 3 provides the centre of expertise for the engineering, testing and evaluation of ICT security techniques and mechanisms within JTC 1.

The scope of WG 3 includes the development and maintenance of standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. This includes consideration of computer networks, distributed systems, associated application services, biometrics, etc.

The scope of WG 3 includes:

- 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.

WG 3 collaborates with other Working Groups in SC 27, in particular with WG 2 on specific cryptographic techniques and WG 5 on identity management, biometrics and protection of personal data.

WG 3 develops and maintains the WG 3 standing documents.

WG 3 ensures liaison and collaboration with those organisations and committees dealing with specific requirements related to security functionality and assurance.

3.4 WG 4 – Security Controls and Services

The scope of WG 4 covers the development and maintenance of standards related to ICT security controls and services and its application to products and systems in information systems, as well as the security in the lifecycle of such products and systems. The standards support the implementation of control objectives and controls as defined in ISO/IEC 27001.

This includes:

- ICT security operations (for example readiness, continuity, incident and event management, investigation)
- Information lifecycle (for example creation, processing, storage, transmission and disposal)
- Organisational 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, virtualisation, storage).

WG 4 collaborates with other Working Groups in SC 27, in particular with WG 1 on ISMS standards and guidelines.

WG 4 develops and maintains the WG 4 standing documents.

WG 4 ensures liaison and collaboration with those organisations and committees dealing

with specific requirements for services and applications.

3.5 WG 5 – Identity Management and Privacy Technologies

The scope of SC 27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

This includes:

- Identity Management, covering role based access control; provisioning; identifiers and single sign-on;
- Privacy covering a privacy framework and reference architecture; privacy infrastructures; anonymity and credentials; Specific Privacy Enhancing Technologies (PETs) and privacy engineering;
- Biometrics, covering protection of biometric data and authentication techniques.
- Identification of requirements for and development of future standards and guidelines in these areas.

WG 5 collaborates with other Working Groups in SC 27, in particular with WG 1 on management aspects, WG 2 on specific cryptographic techniques and WG 3 on evaluation aspects.

WG 5 develops and maintains the WG 5 standing documents.

WG 5 ensures liaison and collaboration with those organisations and committees dealing with specific requirements for identity management, biometrics and the protection of personal data.

4 Advisory Group on Management (MAG)

The Advisory Group operates under the direction of SC 27 Management to review and evaluate the effectiveness of SC 27 and to make recommendations to SC 27 Management [1] to this effect.

This includes:

- Review, audit and evaluate the structure and management processes in SC 27 and develop recommendations for improvements;

[1] This refers to the SC 27 Chair, Vice Chair, Secretariat, Working Group Convenors and Vice Convenors

- Explore alternatives for the meeting structures (Plenary and Working Groups) and agenda of the SC 27 Plenary meetings;
- Provide advice on matters of operational efficiency;
- Advise and review of tools used to support the SC 27 processes;
- Review of the effective distribution of public information on SC 27 activities and propose suggestions for improvements;
- Provide advice, help and guidance to SC 27 Management on standards management and development;
- Serve as an appeal body in case of an arbitration request from an SC27 member or Officer;
- Monitor the activities, reports and recommendations of the JTC 1 Advisory Group (JAG);
- Periodically report results and recommendations to SC 27 Management and coordinate ongoing work with related plans prior to the SC 27 Plenary meetings.

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

Administration

The Advisory Group will be managed by a Convenor, supported by a Vice-Convener, under approval of the SC 27 Management and endorsement by the SC 27 Plenary. The Advisory Group management is responsible for the administration of the group.

Membership and composition

Membership will consist of a maximum of ten (10) SC 27 members having at least 5, but ideally 10 years' experience within SC 27, preferably as an SC 27 Officer, but shall not include anyone who is a current member of the SC 27 Management (i.e. the SC27 Chair, the SC27 Vice-Chair, the Working Group Convenors and Vice-Convenors). The size of the Advisory Group is kept small enough to communicate and operate effectively.

Members to the Advisory Group shall be nominated by National Bodies or Working Group Convenors but are appointed by the SC 27 Management for a term of three (3) years in agreement with the Advisory Group Management. A statement of motivation shall accompany National Body nominations. The Convenor and Vice-Convenor are elected by the Advisory Group members for a term of three (3) years. Any appointment to the Advisory Group (Convenor, Vice-Convenor or member) can only be renewed once. No alternate is allowed if a member cannot attend a meeting. Any Advisory Group Member not attending two meetings in a row will be subject to replacement.

The Advisory Group membership will contain at least one member from each Working Group and should ensure an appropriate geographical spread. Experts/ guests may be invited to meetings for specific subjects at the discretion of the Advisory Group Convenor.

Modus Operandi

The Advisory Group shall mainly work electronically via e-mail. Regular remote meetings (e.g. Zoom, teleconference) will be organised to progress the work and at least one physical meeting in conjunction with the SC 27 meetings shall be held each half year.

Agendas and minutes (including action points) of the Advisory Group remote or physical meetings shall be prepared in due time and shared with the SC27

Management once agreed by the Group. The Advisory Group shall agree yearly on a list of issues and priorities. Work items will be progressed via written contribution papers / proposals.

Members will be requested to submit written contributions on all topics before each electronic or physical meeting. These contributions will be distributed before each meeting, and the main function of the WebEx meetings will be to agree consensus proposals on those topics that can then be submitted to the SC27 Management.

All MAG internal documents shall be kept private to MAG members, after approval by MAG they will be forwarded as MAG proposals to the SC27 Management for their consideration, the SC 27 Management will decide whether to distribute MAG proposals to SC 27 National Bodies for decision.

The Advisory Group Convenor and Vice-Convenor will be invited to the SC27 Management Coordination meetings.

5 Special Working Group on Transversal Items (SWG-T)

SWG-T operates under the direction of SC 27 to address topics which are beyond the scope of the respective existing WGs or can affect directly or indirectly multiple WGs. SWG-T can make recommendations to the SC 27 Management, to the SC27 Plenary and to the SWG-M to this effect. This includes:

- Identify any gaps in the portfolio of SC 27 standards and projects to ensure market needs are being adequately addressed;
- Alignment and coordination of WG roadmaps and overall SC 27 roadmap;
- Harmonisation of vocabulary;
- Review of issues arising from overlapping / conflicting scopes, activities and projects as well as disagreement on project assignments between Working Groups and beyond. SWG-T shall work with SC 27 Working Group Conveners and Liaison Officers to identify issues and to reach acceptable resolutions;
- Adherence to scope for projects under development and monitoring of project progress with related work programmes / plans and regularly report results and

recommendations to SC 27;

- Review proposals and provide advice to SC 27 on initiatives such as Study Groups,
- New Work Item Proposals (NWIPs), Fast-Tracks, and PAS submissions;
- Monitor progress of SC 27 Study Groups;
- SC 27 liaisons and common topics with other SCs or Standardization Bodies.

The SWG-T functions purely in an advisory capacity to the SC 27 Management and SC 27 Plenary.

Composition of SC 27 Management Advisory Group (MAG)

The composition [1] of the MAG is as follows:

MAG Convenor	
Jean-Pierre Quémard **AFNOR / FRANCE**	E-mail: jean-pierre.quemard@kat.bzh
MAG Vice-Convenor	
Mike Nash **BSI / UNITED KINGDOM**	E-mail: mnash@gammassl.co.uk
MAG Members	
Jinghua Min, WG 4 **SAC / CHINA**	E-mail: minjinghua@cecgw.cn
Nat Sakimura, WG 5 **JISC / JAPAN**	E-mail: nat@sakimura.org
Taewan Park, WG 1 **KATS / KOREA**	E-mail: taewan.park@outlook.com
Benoit Poletti, WG 4 **INLAS / LUXEMBOURG**	E-mail: incert.lux@gmail.com
Hans Hedbom, WG 5 **SIS / SWEDEN**	E-mail: hans.hedbom@kau.se
Chris Mitchell, WG 2 **BSI / UNITED KINGDOM**	E-mail: me@chrismitchell.net

[1] As per Recommendation 2 (contained in N17810) of SC 27 HoD Meeting in Berlin, Germany, 2017-11-02.