ISO/IEC JTC 1/SC 27 N20000

REPLACES: N19620

ISO/IEC JTC 1/SC 27

Information security, cybersecurity and privacy protection

Secretariat: DIN, Germany

DOC TYPE:	**officers' contribution**
TITLE:	**Welcome package of ISO/IEC JTC 1/SC 27 -- Information security, cybersecurity and privacy protection**
SOURCE:	**JTC 1/SC 27 Committee Manager**
DATE:	**2019-10-11**
PROJECT:	
STATUS:	**This document is circulated for information.**
PLEASE NOTE:	**This document is also freely accessible from the public SC 27 website at: http://www.din.de/go/jtc1sc27 "Downloads"**
ACTION ID:	**INFO**
DUE DATE:	
DISTRIBUTION:	**P-, L-, O-Members A. Wolf, SC 27 Chairman L. Lindsay, SC 27 Vice-Chair E. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG Convenors**
MEDIUM:	**http://isotc.iso.org/livelink/livelink/open/jtc1sc27**
NO. OF PAGES:	**1 + 94**

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e. V., Saatwinkler Damm 42/43, D-13627 (postal D-10772) Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-42652; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27
Information Security, Cybersecurity and Privacy Protection
WELCOME PACKAGE 2019

(September 2019)

http://www.din.de/go/jtc1sc27

SC 27 Mission

The development of standards for information security, cybersecurity and privacy protection. 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 systems (ISMS), 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;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

SC 27 Structure

SC 27 Chairman: DIN, Germany, Dr. Andreas Wolf
SC 27 Vice-Chair: ANSI, United States, Laura Lindsay
SC 27 Communications Officer: BSI, UK, Dr. Edward Humphreys
SC 27 Committee Manager: DIN, Germany, Krystyna Passia
SC 27 Secretariat: DIN, Germany

SC 27 Structure

WG 1: Information Security Management Systems

- Convenor: Prof. Dr. Edward Humphreys, BSI, UK,
- Vice-Convener: Pablo Corona, DGN, Mexico

WG 2: Cryptography and Security Mechanisms

- Convenor: Takeshi Chikazawa, JISC, Japan
- Vice-Convener: Hirotaka Yoshida, JISC, Japan

WG 3: Security Evaluation, Testing and Specification

- Convenor: Miguel Bañón, UNE, Spain
- Vice-Convener: Naruki Kai, JISC, Japan

SC 27 Structure

WG 4: Security Controls and Services

- Convenor: Johann Amsenga, ILNAS, Luxembourg
- Vice-Convener: François Lorek, AFNOR, France

WG 5: Identity Management and Privacy Technologies

- Convenor: Prof. Dr. Kai Rannenberg, DIN, Germany
- Vice-Convener: Dr. Jan Schallaböck, DIN, Germany

SC 27 Structure

SC 27 Management Advisory Group (MAG)

- Convenor: Jean-Pierre Quémard, AFNOR, France
- Vice-Convenor: Dr. Mike Nash, BIS, United Kingdom

Special Working Group on Transversal Items (SWG-T)

- Convenor: Dr. Andreas Fuchsberger, DIN, Germany

SC 27 Structure

Study Group on Data Security

- Convenors: Laura Lindsay, ANSI, United States
- Vice-Convenor: Yan Sun, SAC, China

Study Group on Trustworthiness

- Convenor: Johann Amsenga, ILNAS, Luxembourg
- Vice-Convenor: Faud Khan, SCC, Canada

Study Group on Concepts and Terminology (SG-CT)

- Convenor: Joanne Knight, NZSO, New Zealand
- Vice-Convenor: Elżbieta Andrukiewicz, PKN, Poland

Security and Privacy Topic Areas

Information security management system (ISMS) requirements *plus*

ISMS supporting guidance - codes of practice of information security controls, ISMS risk management, ISMS performance evaluation and ISMS implementation guidance

ISMS sector specific security controls *(including application and sector specific e.g. Cloud, Telecoms, Energy, Finance)* **and sector-specific use of ISMS requirements standard**

Security services and controls *(focusing on contributing to security controls and mechanisms, covering ICT readiness for business continuity, IT network security, 3rd party services, supplier relationships (including Cloud), IDS, incident management, cyber security, application security, disaster recovery, forensics, digital redaction, time-stamping and other areas)*

Identity management and privacy technologies *(including application specific (e.g. cloud and PII), privacy impact analysis, privcy framework, identity management framework, entity authentication assurance framework, biometric information protection, biometric authentication)*

ISMS accreditation, certification and auditing *(including acreddited CB requirements, guidance on ISMS auditong and guidelines for auditors on ISMS controls)*

Security Evaluation, Testing and Specification *(including evaluation criteria for IT security, framework for IT security assurance, methodology for IT security evaluation, cryptographic algorithms and security mechanisms conformance testing, security assessment of operational systems, SSE-CMM, vulnerability disclosure, vulnerability handling processes, physical security attacks, mitigation techniques and security requirements)*

Cryptographic and security mechanisms *(including encryption, digital signature, authentication mechansisms, data integrity, non-repudiation, key management, prime number generation, random number generation, hash functions)*

(SC 27 WELCOME PACKAGE 2019-09)

Projects Facts & Figures
Standing Documents

- Projects
  - Total no of projects: 270
  - No of active projects: 82
  - Current number of published standards: 188
- Standing Documents (all freely available from the SC27 site as given below)
  - SD6 Glossary of IT Security terminology (http://www.din.de/go/jtc1sc27)
  - SD7 Catalogue of SC 27 Projects and Standards (http://www.din.de/go/jtc1sc27)
  - SD11 Overview of SC 27 (http://www.din.de/go/jtc1sc27)
  - SD12 Assessment of cryptographic algorithms and key lengths (http://www.jtc1sc27.din.de/sbe/SD12)

Projects Facts & Figures (2)
Standing Documents

- Standing Documents (all freely available from the SC27 site as given below)
  - SD13 Best practices guide for use of WG Livelink (http://www.din.de/go/jtc1sc27 / Downloads)
  - SD14 Transversal item handling
  - SD15 Scope alignment on SC 27 transversal projects
  - SD16 Information security library (http://www.din.de/go/jtc1sc27 / Downloads)
  - SD17 SC 27 Guide for editors
  - SD18 SC 27 Structure and scope (http://www.din.de/go/jtc1sc27 / Downloads)
  - SD19 Risk management resource library (RL) (ver. 1.0) (http://www.din.de/go/jtc1sc27 / Downloads)
  - SD20 List of Liaison Representatives to and from ISO/IEC JTC 1/SC 27

SC27 Members

Products in SC 27 are developed by experts from members bodies.

- *Experts come from the industrial, technical and business sectors which require and use IT security standards*
- *Member bodies consists mostly of National Bodies representing countries*

Membership types:

- *Participating (P-Members)*
- *Observing (O-Members)*
- *Liaison (L-members)*

Participating Members *(P-Members)*

- ISO/IEC member bodies which wish to play an active role in the work of SC 27.
- These members have
  - *an obligation to vote on the progress of projects in SC 27; and*
  - *a duty to identify experts who may be able to contribute to the related working group activities.*

The P-members are:

Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Denmark, Estonia, Finland, France, Germany, India, Indonesia, Ireland, Islamic Rep, of Iran, Israel, Italy, Japan, Rep. of Korea, Lebanon, Luxembourg, Malaysia, Mauritius, Mexico, The Netherlands, New Zealand, Norway, Panama, Peru, Poland, Romania, Russian Federation, Saint Kitts and Nevis, Singapore, Slovakia, South Africa, Sri Lanka, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay (Total: 49)

Observing members (*O-Members*)

- ISO/IEC member bodies who wish to follow the development of a product in SC 27, and possibly to make contributions to the work, without committing themselves to active participation.

The O-members are:

Belarus, Bosnia and Herzegovina, Bulgaria, Chile, Cote d'Ivoire, Czech Republic, El Salvador, , Eswatini, Ghana, Hong Kong, Hungary, Iceland, Kazakhstan, Kenya, Lithuania, Morocco, North Macedonia, Pakistan, Philippines, Portugal, Rwanda, State of Palestine, Saudi Arabia, Senegal, Serbia, Slovenia, Thailand, Trinidad and Tobago, Turkey (Total: 29)

Liaison Partners (1)
Internal liaisons

- Internal liaisons are technical committees or subcommittees in ISO and IEC working in related fields, typically those
  - *being influenced by the products of SC 27, such as security of financial services;*
  - *having an impact on projects in SC 27, such as coordination on management system standards; and*
  - *work in areas*
- Internal liaisons contribute to discussions in meetings through liaison officers.
- Internal liaisons contribute through submission of written comments, on matters within the competence of their own technical committee.

Liaison Partners
External liaisons

- Liaison Cat A organisations make an effective contribution to the work of SC 27 on committee level. These organisations may nominate experts to participate.
  - *Examples are organisations focussing on cloud security, financial information security, and international organisations addressing information security in general.*
- Liaison Cat C organisations make an effective technical contribution and participate actively at the working group or project level of SC 27.
  - *Examples are organisations that focusses on areas specific to one or more SC 27 working groups, such as privacy, telecommunications, evaluation of security services, systems and products, and incident response.*

SC 27 Liaison Partners

Internal Liaisons within ISO

- *ISO/CASCO*
- *International Accreditation Forum (IAF)*
- *ISO/JTCG Joint technical Coordination Group on MSS*
- *ISO/TC 8 Ships and marine technology*
- *ISO/TC 22/SC 31 Road vehicles -- Data communication*
- *ISO/TC 22/SC 32 Road vehicles -- Electrical and electronic components and general system aspects*
- *ISO/TC 46/SC 11 Information and documentation – Archives/Records management*
- *ISO/TC 68/SC 2 Financial services – Security*
- *ISO/TC 176/SC 3 - Quality management and quality assurance - Supporting technologies*
- *ISO/TC 176/SC 3/WG 16 Quality management and quality assurance - Supporting technologies - Joint WG with TC 207/SC2 for the revision of ISO 19011*
- *ISO/TC 204 Intelligent transport systems - WG 1 Architecture*
- *ISO/TC 208 Thermal turbines for industrial application (steam turbines, gas expansion turbines)*

SC 27 Liaison Partners

Internal Liaisons within ISO

- *ISO/TC 46/SC 11 Information and documentation – Archives/Records management*
- *ISO/TC 68/SC 2 Financial services -- Security*
- *ISO/TC 171 Document management applications*
- *ISO/TC 176/SC 3 - Quality management and quality assurance - Supporting technologies*
- *ISO/TC 204 Intelligent transport systems - WG 1 Architecture*
- *ISO/TC 208 Thermal turbines for industrial application (steam turbines, gas expansion turbines)*
- *ISO/TC 215 Health informatics - WG 4 Security*
- *ISO/TC 251 Asset management*
- *ISO TC 259 Outsourcing*
- *ISO/TC 262 Risk management*
- *ISO/TC 272 Forensic sciences*
- *ISO/TC 292 Security and resilience*
- *ISO/TC 307 Blockchain and distributed ledger technologies*

SC 27 Liaison Partners

Internal Liaisons within ISO

- *ISO/TC 309 Governance of organizations*
- *ISO PC 317 Consumer protection: Privacy by design for consumer goods and service*

Internal Liaisons within IEC

- *IEC/TC 45/SC 45A Instrumentation, control and electrical systems of nuclear facilities*
- *IEC SG 9 Smart home /Office building systems*
- *IEC/SC 121A Low-voltage switchgear and controlgear*
- *IEC/TC 57 Power systems management and associated information exchange - WG 15 Data and communication security*
- *IEC/TC 65 Industrial-process measurement, control and automation – WG 10 Security for industrial process measurement and control – Network and system security*

SC 27 Liaison Partners

Internal Liaisons within ISO/IEC JTC 1

- *JTC 1/WG 11 Smart cities*
- *SC 6 Telecommunications and information exchange between system*
- *SC 7 Software and systems engineering*
- *SC 17 Cards and security devices for personal identification*
- *SC 17/WG 3 Machine readable travel documents*
- *SC 17/WG 4 Integrated circuit cards with contacts*
- *SC 17/WG 11 Application of biometrics to cards and personal identification*
- *SC 22 Programming languages, their environments and system software interfaces*
- *SC 25 Interconnection of IT equipment*
- *SC 29/WG 1 Coding of Audio, Picture, Multimedia and Hypermedia Information – Coding of Still Pictures*
- *SC 31/WG 7 Automatic identification and data capture techniques -- Radio frequency identification for item management*
- *SC 32 Data management and interchange*
- *SC 37 Biometrics*
- *SC 38 Cloud Computing and Distributed Platforms*
- *SC 40 IT service management and IT governance*

SC 27 Liaison Partners

Internal Liaisons within ISO/IEC JTC 1

- *JTC 1/WG 11 Smart cities*
- *SC 41 Internet of Things and related technologies*
- *SC 42 Artificial Intelligence*

SC 27 Liaison Partners

External CAT A Liaisons L SEP

- *Calendaring and Scheduling Consortium (CallConnect)*
- *Cloud Computing Association (CSA)*
- *ECMA International*
- *European Network and Information Security Agency (ENISA)*
- *European Payment Council (EPC)*
- *European Telecommunications Standards Institute (ETSI)*
- *ETSI TC CYBER (ISG ISI / MTS /TC ESI/ NFV)*
- *Global Platform*
- *Information Systems Audit and Control Association/IT Governance Institute (ISACA/ITGI)*
- *International System Security Certification Consortium (ISC)2*
- *ITU-T Joint coordination activity on identity management (JCA-IdM)*
- *ITU-T SG 13 (Study Group 13 – Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures)*
- *ITU-T SG 17 (Study Group 17 -- Security)*

SC27 Liaison Partners

External CAT A Liaisons

- *ITU-T SG 20 (Study Group 20 -- IoT and its applications including smart cities and communities (SC&C))*
- *MasterCard*
- *Small Business Standards*

External CAT C Liaisons

- *ABC4Trust*
- *European Data Protection Board (EDPB)*
- *Common Criteria Development Board (CCDB)*
- *CREDENTIAL (seCuRE clouD idENTIty wALlet)*
- *Cyber Security Naming and Information Structure Group Corporation (CSNISG)*
- *Forum of Incident Response and Security Teams (FIRST)*
- *Information Security Forum (ISF)*
- *Instituto Latinoamericano de Aseguramiento de la Calidad A. C. (INLAC) (The Latin-American Institute for Quality Assurance A.C.)*
- *ISA99*
- *International Conference of Data Protection and Privacy Commissioners*
- *International Smart Card Certification Initiatives*

SC 27 Liaison Partners

External CAT C Liaisons L SEP

- *Interpol*
- *Kantara Initiative*
- *OASIS*
- *OECD*
- *PQCRYPTO*
- *PRIPARE (FP7 Project)*
- *PRISMACLOUD*
- *Privacy and Identity Management for Community Services (PICOS)*
- *SAFEcrypto*
- *Technology-supported Risk Estimation by Predictive Assessment of Sociotechnical Security (TREsPASS)*
- *The Open Group*
- *The OpenID Foundation*
- *Trusted Computing Group (TCG)*

SC 27 Liaison Partners

External liaisons Under Vienna Agreement

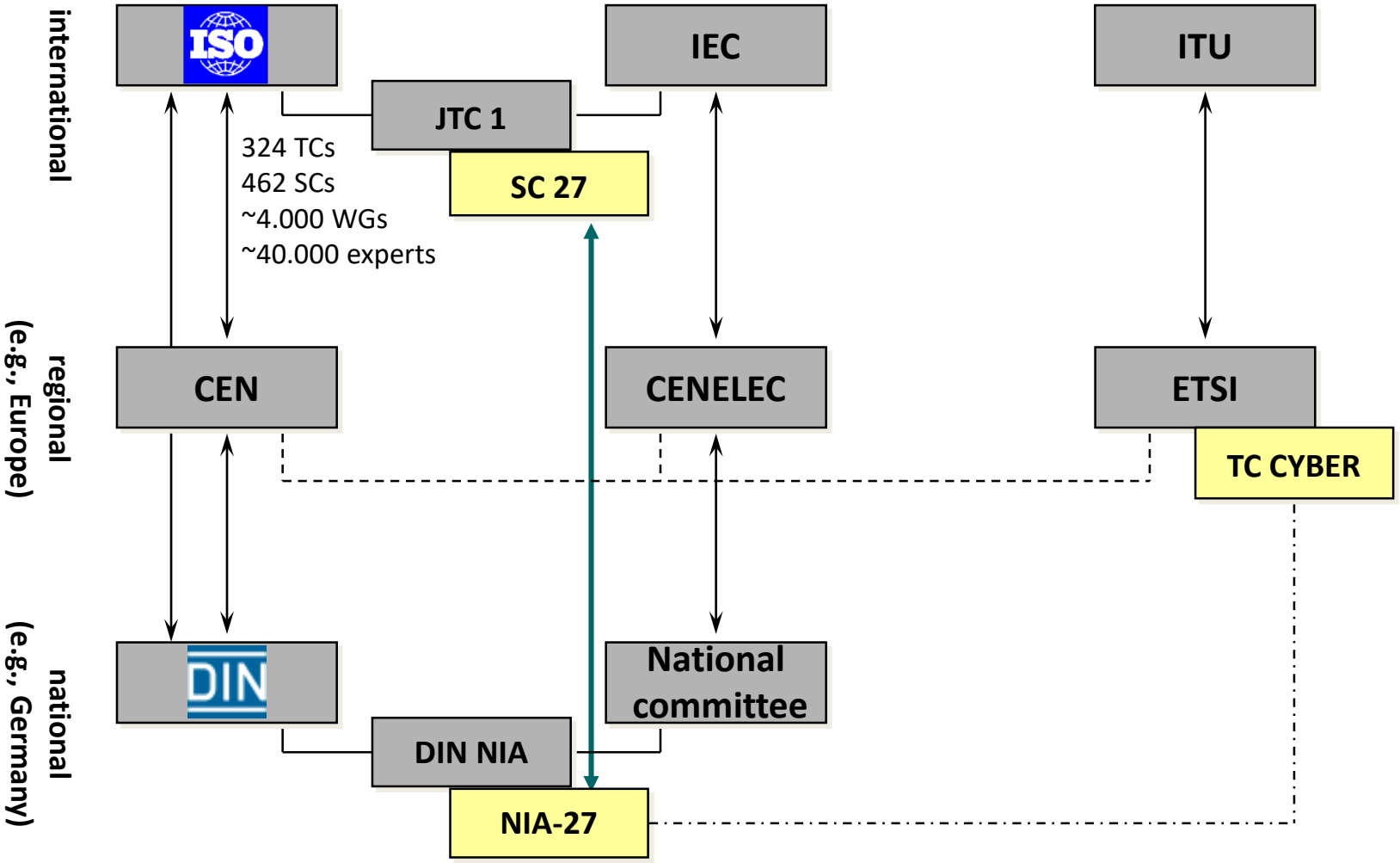
- *CEN/CENELEC JTC 13 (Cybersecurity and data protection)*
- *CEN/TC 224 Personal identification, electronic signature and cards and their related systems and operations*
- *CEN/TC 377 Air Traffic Management*
- *CEN/TC 428 e-Competences and ICT professionalism*

SC 27 within ISO (1)

www.iso.org /All about ISO (2019-09-25)

- ISO: International Organization for Standardization
- Worldwide federation of national standards bodies from 146 countries, one from each country, e.g.,
  - IBN - Institut Belge de Normalisation (Belgium)
- ISO was established in 1947 (www.iso.ch)
- Mission
  - to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity.
- 3.493 technical bodies
  - 324 technical committees (TCs)
  - 462 subcommittees (SCs)
  - 3175 working groups (WGs)
- ISO's work results in international agreements which are published as International Standards (IS)
  - 22572 standards and standards-type documents
  - 100 published new International standards each month

SC27 within ISO/IEC Interconnections (2)



(SC 27 WELCOME PACKAGE 2019-09)

SC 27 within ISO/IEC JTC 1 (3)

General Information for Members of JTC 1 and its Sub-Committees

- **ISO/IEC JTC 1 offers its public website accessible at www.iso.org/ittf**

This website provides the following information

- **Mission of JTC 1**
- **Promoting material**
  - **JTC 1 Vision, Mission and Principles**
  - **JTC 1 Business Plan**
  - **Achievements**
  - **JTC 1 facts and figures**
  - **JTC 1 releases preliminary reports on emerging areas of work:**
    - **Big Data (Preliminary Report 2014)**
    - **Internet of Things (Preliminary Report 2014)**
    - **Smart cities (Preliminary Report 2014)**

SC 27 within ISO (4)

General Information for Members of JTC 1 and its Sub-Committees
ISO/IEC JTC 1 offers its public website accessible at www.iso.org/ittf
In addition, this website provides the following useful links

- **Resources**
  - **Meeting calendar https://sd.iso.org/meetings**
  - **Publicly Available standards https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html**
  - **Resources for standards development (including Directives, templates and IT tools) https://www.iso.org/resources.html**
  - **ISO project portal https://sd.iso.org/projects**
  - **Patents database https://www.iso.org/iso-standards-and-patents.html**
  - **JTC1 Stabilized Standards (excel file) https://www.iso.org/isoiec-jtc-1.html**
  - **History of JTC1 (external link) https://jtc1historyblog.wordpress.com/**
  - **Structure of ISO/IEC JTC 1 https://jtc1info.org/**

SC 27 within ISO/IEC JTC 1 (5)

Working area publicly accessible for members of JTC 1 and its sub-committees (SCs) (e-committee on ISO Livelink Platform): www.iso.org/jtc1

- **This area offers:**
  - **JTC 1 and its sub-committees Business Plans**
  - **Procedural material**
    - ✓ **JTC 1 Consolidated Supplement – Procedures specific to JTC 1, edition 2018 (see also www.iso.org/directives)**
    - ✓ **Standing Documents**
    - ✓ **Templates**
    - ✓ **Forms (see also www.iso.org/forms)**

Working area with restricted access (password-protected) accessible at the following URL:

- **For JTC 1 http://isotc.iso.org/livelink/livelink/open/jtc1**
- **For JTC 1/SCs (e.g. SC 27) http://isotc.iso.org/livelink/livelink/open/jtc1sc27**

SC 27 within ISO/IEC (6)

General Information on ISO

- General information at: www.iso.org on
- ISO Code of Conduct https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100397.pdf
  (Implementation suggestions for ISO Code of Conduct
  http://www.iso.org/iso/suggestions_for_implementation_of_the_iso_code_of_conduct.pdf)
- Standards http://www.iso.org/iso/home/standards.htm
  (benefits, certification, management system standards, education about standards)
- About ISO http://www.iso.org/iso/home/about.htm
  (structure, members, consumers, conformity assessment, developing countries, training)
- Standards development http://www.iso.org/iso/home/standards_development.htm (technical committees, deliverables, who develops standards, why get involved?, resource area)
- News http://www.iso.org/iso/home/news_index.htm
  (ISO standards in action, ISO Magazines, events, media Kit)
- ISO store http://www.iso.org/iso/home/store.htm

ISO processes – How to become an SC 27 member

How to become a member as

- P-member (actively participating)

Any national body with status of a "member body of ISO"

  - More information can be found at: http://www.iso.org/iso/home/about/iso_members.htm

- O-member (observer)

Any national body with status of a „member body of ISO"

  - More information can be found at: http://www.iso.org/iso/home/about/iso_members.htm

Contact:

- ISO/Central Secretariat (ITTF) at: helpdesk@iso.org or
- SC 27 secretariat at: krystyna.passia@din.de

Note: any P- or O-member of SC 27 must be at least O-member of JTC 1

ISO processes – How to become an internal liaison member (1)

Within **INTERNAL** liaisons the following categories are possible:

- **INTERNAL** within
  - **ISO** (liaisonship is established at the Technical Committee (TC) or Sub-committee (SC) level or between SCs)
  - **IEC** (liaisonship is established at the Technical Committee (TC) or Sub-committee (SC) level or between SCs of both ISO and IEC)
  - **ISO/IEC JTC 1** (liaisonship is established at the Technical Committee (TC) or Sub-committee (SC) level or between SCs)

ESTABLISHMENT

As per Resolution of a Technical Committee / Sub-committe concerned

- Either at the TC / SC Plenary
- Or by correspondence via a 4-week default ballot

REGISTRATION

Once approved the applying TC/SC requests the target TC/SC to register its liaison representatives via the ISO/TC Support to update the ISO Global Directory accordingly.

ISO processes – How to become a external liaison member (2)

Within EXTERNAL liaisons the following categories are possible:

- **EXTERNAL**
  - **Category A**
    - ✓Area of interest/cooperation: SC 27 programme of work as whole (at the technical committee or subcommittee level
  - **Category C**
    - ✓(Area of interest/cooperation is related to a particular project or a working group (at the working group level
  - **Under Vienna Agreement (CEN, CENELEC)**
    - ✓Area of interest/cooperation: SC 27 programme of work as whole (at the technical committee / subcommittee / working group level)

NOTE: ESTABLISHMENT of external liasions between CEN, CENELEC and ISO or or JTC 1 is simpliefied as per the VIENNA AGREEMENT and is APPROVED

- **As per Resolution of a Technical Committee / Sub-committe concerned**
  - **Either at the TC / SC Plenary**
  - **Or by correspondence via a 4-week default ballot**
  - **No ENDORSEMENT by a parent body required!**

(SC 27 WELCOME PACKAGE 2019-09)

ISO processes – How to become an external liaison member (3)

ESTABLISHMENT:

- **Submission of an application form (to be downloaded from www.iso.org /forms) directly to the SC 27 secretariat for further forwarding to the ISO/CS (ITTF) to validate the eligibility criteria. The applicant confirms that the organization is:**
  - **is not for profit;**
  - **is a legal entity (NOTE: this is a requirement only for Category A liaisons);**
  - **is membership-based and open to members worldwide or over a broad region;**
  - **through its activities and membership demonstrates that it has the competence and expertise to contribute to the development of International Standards or the authority to promote their implementation;**
  - **has a process for stakeholder engagement and consensus decision-making to develop the input it provides (see Guidance for ISO liaison organizations — Engaging stakeholders and building consensus http://www.iso.org/iso/guidance_liaison-organizations.pdf).**
- **The applicant must also provide justification (e. g. reason, benefit for both sides, to actively contribute to the SC 27 programme of work), a name(s) of liaison representatives, category of a liaison (for details see next page).**

  Once the application APPROVED by ITTF two-level approval process within JTC 1 applies:
  - **At SC 27 level via a 4-week default ballot and subsequently (once approved)**
  - **At JTC 1 level via a 4-week default ballot**
- **If approved ISO/CS (ITTF) issues an official notification of the new external liaison establishment and registers the liaison representatives as SC 27 liaison members.**

ISO processes – How to become an external liaison organization (4)

Status of external liaison organizations

- Category A
  - » Access to documents at committee/subcommitte and working group levels;
  - » Participation in regular and special meetings of SC 27 and its working groups;
  - » Submit comments via the e-balloting website (technical committee or subcommittee level)
  - » The right to submit new work item proposals (NP);
  - » The right to submit JTC 1 Fast Track documents.
- Category C
  - » Access to documents at working group level;
  - » Participation in regular and special meetings of SC 27 working groups;
  - » Submit comments directly either via the so called **WG Consultation Application** * or directly to sc secretariat .

For more information refer to JTC 1 SD15 on liaisons www.iso.org/ittf

*** All liaison experts must be registered with the ISO/CS via the ISO Global Directory. For this purpose please contact the SC 27 secretariat at krystyna.passia@din.de**

ISO processes – Electronic applications (1)

FREELY ACCESSIBLE ISO electronic applications provided by the ISO/CS (ITTF) :

- **Online Browsing Platform (OBP): Access the most up to date content on ISO standards: http://www.iso.org/obp**

  The following parts of a published product (International Standard (IS), Technical Specification (TS), Technical Report (TR) can be obtained from the OBP at no cost:

  - **Table of Contents, Foreword, Introduction, Scope, Terms and Definitions**

- **RESOLUTIONS of ISO TECHNICAL MANAGEMENT BOARD (TMB): Access the TMB Resolutions most recent and those of past Plenary meetings: www.iso.orgTMBResolutions**
- **ISO TMB COMMUNIQUES:**

  - **http://isotc.iso.org/livelink/livelink?func=ll&objId=15788626&objAction=browse&viewType=1)**

ISO processes – Electronic applications (2)

ACCESSIBLE FOR MEMBERS ONLY (by single login) at: https://login.iso.org

- **Event Notifications**: Manage notification reports on changes in the ISO system.
- **Electronic Balloting**: Support of consensus feedback processes in ISO standardization (URL: https://isotc.iso.org/livelink/eb3/home.do)
- **Global Directory**: Central repository for managing committees, organizations, users and their roles for international, regional, and national work.
- **ISO TC Server**: Document management systems for the collaborative development of standards (https://isotc.iso.org/livelink/livelink)
- **Meeting Portal**: Support ISO committees meetings organization (URL: https://sd.iso.org/meetings)
- **Project Portal**: Aggregated project status information for ISO committees and member bodies (URL: https://sd.iso.org/projects)
- **Submission Interface**: Support of file and project data submissions to the ISO Central Secretariat (URL: https://isotc.iso.org/livelink/si/home.do)
- **National Mirror Committees**: Dissemination of ISO documents to National Mirror Committees.
- **Zoom:** The ISO tele-conferencing application

ISO processes – Electronic applications (3)

Electronic applications for use by SC 27 members

IMPORTANT: In the event of any problems (for all ISO applications) **please contact: helpdesk@iso.org and NOT the SC 27 Secretariat**

– **LIVELINK** – for electronic document distribution accessible at:

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

Within SC 27 document distribution is (currently) provided at the sub-committee level.

This means:

a) **All documents (either „WG-specific“ or „sub-committee-specific)** are maintained at the sub-committee level,

b) **Access** is granted to users registered as a „committee member“ by a National Body (national GD administrator) concerned via the ISO Global Directory; there is no access for WG members (WG experts).

For more information, see ISO eCommittee Guide for Committee Members and Experts:
www.iso.org/e-guides

ISO processes – Electronic applications (4)

Electronic applications for use by SC 27 members

- **Committee Internal e-Balloting (CIB)** application accessible at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

  /Committee ballots (navigation menu)

  a) **Administrates committee-internal balloting** which means for committe-specific documents (e.g., ballots on NP, CD, PDTR, PDTS, etc.)

  b) **Registration as „committee balloter“ ONLY** by a National Body (national GD administrator) concerned via the ISO Global Directory

  c) **Registration as „commenter“ ONLY for O-members and liaisons CAT A** by the ISO/CS (ITTF); assigned automatically when membership/liaison is established

For more information, see Guide for committee-internal balloting - for Committee members : www.iso.org/e-guides

ISO processes – Electronic applications (5)

Use of Committee Internal e-Balloting (CIB) as „Commenting website“ within SC 27 (ONLY for documents with NO OBLIGATION TO SUBMIT RESPONSES)

a) **Administrates submissions of comments/contributions/any other National Body responses** which means for specific documents (e.g. calls for contributions to SC 27-level study periods, call a liaison officer, nomination of editors, etc.)

b) **Registration as „committee balloter“ ONLY** by a National Body (national GD administrator) concerned via the ISO Global Directory

c) **Registration as „commenter“ ONLY for O-members and liaisons CAT A** by the ISO/CS (ITTF); assigned automatically when membership/liaison is established

ISO processes – Electronic applications (6)

- **E-balloting for DIS/FDIS administrated by ISO/CS (ITTF)**
  - **a) Access**
    - i. either through ISO electronic applications homepage at https://login.iso.org
    - ii. or through directly from the SC 27 homepage at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27 /Committee ballots (navigation menu)
  - **b) Administrates balloting for documents under the direct responsibility of the committee / sub-committee concerned** (e.g. ballots on DIS/FDIS, fast-track DIS/FDIS)
  - **c) Regisitration as a „balloter“ ONLY** by a National Body (national GD administrator) concerned via the ISO Global Directory

For more information, see Guide on Electronic Balloting on DIS and FDIS in ISO: www.iso.org/e-guides

ISO processes – Electronic applications (7)

- **E-balloting for Systematic Review (SR) administrated by ISO/CS (ITTF)**
  - **a) Access**
    - i. either through ISO electronic applications homepage at https://login.iso.org
    - ii. or through directly from the SC 27 homepage at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27 /Committee ballots (navigation menue)
  - **b) Administrates balloting** of published documents (International Standards, Technical Specifications); lauched every 5 years after publication.
  - **c) Registration as a „balloter“ ONLY** by a National Body (national GD administrator) concerned via the ISO Global Directory.

For more information, see Guide on Electronic Balloting on DIS and FDIS in ISO: www.iso.org/e-guides

ISO processes – Electronic applications (8)

- **E-balloting administrated by JTC 1** (JTC 1 balloter)
  a) **Access** directly from the JTC 1 homepage at: http://isotc.iso.org/livelink/livelink/open/jtc1
     /Committee ballots (navigation menu)
  b) **Administrates balloting for documents being maintained at JTC 1 level** (e.g., ballots on NP, fast-track DTR/DTS)
  c) **Registration as a „JTC 1 balloter“ ONLY** by a National Body (contact national GD administrator at www.din.de/go/jtc1sc27 / members) concerned via the ISO Global Directory

For more information, see Guide for committee-internal balloting – for Committee members: www.iso.org/e-guides

ISO processes – Electronic applications (9)

ISOTC Livelink for Working Groups

- **LIVELINK** – for electronic document distribution accessible at:

http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3 for WG 3
http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4 for WG 4

- **Registration/Access**
  - » WG experts need to get registered by a National Body concerned via the ISO Global Directory (contact the national GD administrator at www.din.de/go/jtc1sc27 / members)
  - » WG liaison representative need to contact the ISO Central Secretariat (helpdesk@iso.og) to get registered for a WG concerned.
- **Document distribution (within a WG) applies for:**
  - » All WG-specific documents which are: Working Drafts, WG standing documents, reports related to WG study periods, expert contributions, call for contribution/exprts/editors/rapporteurs, all other documents related to any activity at a WG-level.
  - » All those WG-level documents related to projects assigned to a WG concerned.

ISO processes – Electronic applications (10)

ISOTC Livelink for Working Groups – WG Consultation Application

- **Purpose**
  - » For WG experts it provides a tool to **directly** submit their responses to any requests for contributions / comments that are launched by a WG management team concerend.
  - » For a WG managment team it provides an adminstrative support to automatically generate a summary of any input materia to be received in response to a request concerned.
- **Registration/Access**

WG experts (both either representing an NB or a liaison organization) who are registered via the ISO global Directory **automatically** get access rights to submit their contributions via the WG Consultation Application.

- **Administration of WG Livelink and WG Consultation Application**

A WG management team has the responsibility to adminster a WG Consultation Apllication.

For more information, see ISO eCommittee Guide for Committee Members and WG Experts: www.iso.org/e-guides

ISO processes – Electronic applications (11)

Zoom: The ISO tele-conferencing application

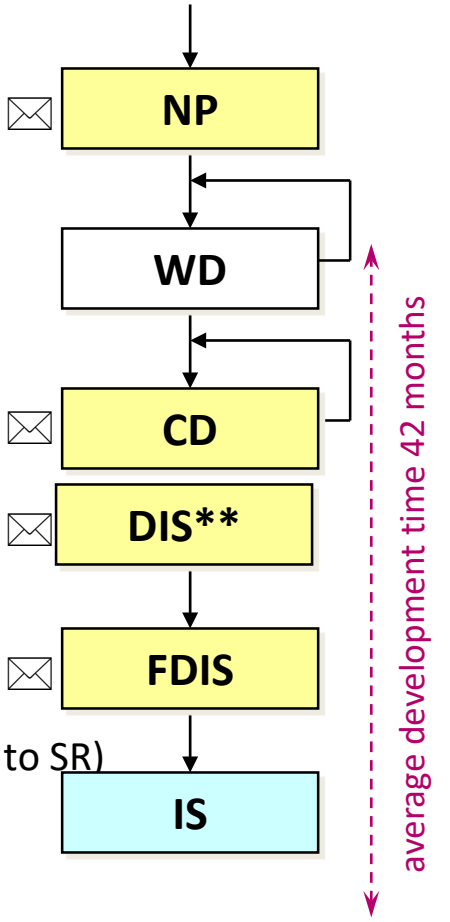
- **Purpose:**
  - For committee officers (chairamen, convenors, committee managers, secretariats, project editors) to provides a tool to **diarrange electronis meeting during and between the regular SC / WG meetings**

- **Registration/Access:**
  - **Contact the WEB CONFERENCING Team at: WEBCONFERENCING@iso.org**

- **ELIGIBILITY CRITERIA are publicly available and can be accessed at:**
  - **https://connect.iso.org/display/it/Eligibility+to+get+an+ISO+Web+Conferencing+account**

ISO processes - Project Development (1)

- Maturity level / state of standardization
  - Study Period / New Project (NP)
    - 3 month NP letter ballot*)
  - Working Draft (WD)
  - Committee Draft (CD)
    - 2*, 3, 4 month CD ballot(s)
  - Draft International Standard (DIS)
    - 3 month DIS ballot (+ 2 months f. translation)
  - Final Draft International Standard (FDIS)
    - 2 month FDIS ballot
    - no more comments at this stage
  - International Standard (IS)
    - pre-review 3 years after publication (subsequent per 2 years prior to SR)
    - review every 5 years (via the Systematic Review at JTC 1 Level)
    - or after 'defect report'



*) Default ballot duration is two months.

**) By 100% approval ONLY (no negative votes and no technical comments received) a FDIS LB can be skipped and the DIS text (after incorporating editorial changes) can be published.

✉ *) one vote per PS member

ISO processes – Project Development (2)

- Projects are developed within editing groups typically chaired by the editor.
- Development is **consensus driven** (no unanimity required) to resolve comments/negative votes.

Consensus may be reached by applying different rules for projects at a WG-level and those that have been elevated to an SC-level. For more details please refer to the subsequent slides**.**

- A Working Group comprises of individual experts (no national body delegations, no national body contributions within a WG)
- Recommendations are reached by a consensus (by simple majority) of the individually participating experts;
- Progression of a project to be elevated from Working Draft (preparatory stage/WG-level) to a Committee Draft (committee stage/SC-level) is recommended by a WG through its Convenor.

PLEASE NOTE: As per Clause 2.4.5 of the JTC 1 Supplement
******As decisions are made regarding the content of the working draft, the Convenor should take care to assure consensus.******

ISO processes – Project Development (4)

b) SUBCOMMITTEE LEVEL

i. For National Body ballot with or without comments e.g. on CDs, DTRs, DISs, etc. (development stages such as committee / enquiry /approval (stage codes 30, 40, 50)) Comment Resolution Meeting (CRM) will be conducted to reach a consnsus as defined by Clauses 2.5, 2.6, 2.7 of the Consolidated JTC 1 Supplement, ed. August 2018);

ii. The CRM is chaired by the respective Project editor (s);

iii. Decision achived by the CRM has a status of a SC 27 Resolution.

Note: The CRM Resolution shall be implemented by the SC 27 Secretariat accordingly.

Balloting rules are laid down in JTC 1 Consolidated Supplement, ed. August 2018 (Annex JA) and ISO/IEC Directives, Part 1, April 2019.

ISO processes - New Work Items (5)

- To evaluate the necessity and the potential of a new work item, a WG may initiate a WG internal preliminary stage (stage code 00) and establish a preliminary work item (PWI) based on written contributions. To further the ideas, the WG may solicit contributions at the WG level or SC 27 level. This stage shall not exceed 2 years with a review performed by the WG after 2 years
- After this period of time the work shall either be abandoned by the WG or the WG shall propose to SC 27 Plenary to initiate an SC 27 preliminary stage, a new work item proposal (NP) or a subdivision of an existing project.
- All proposals to SC 27 shall be accompanied by supporting documentation, including a brief outline of the necessity and potential of the work, as well as the necessary documents in case of an NP (NP, stage code 10 - see the Consolidated JTC 1 Sup.) In addition (see SD5) it shall include as a minimum (preliminary) Working Draft (WD)) or an outline document containing:
  - a proposed table of contents;
  - the proposed scope, elaborated with a rich description of both in-scope and out-of-scope areas, cross-over/conflict with other standards etc, and ideally with a summary diagram such as a mind map;
  - a description of the nature of the material that will be included in each of the major clauses; and
  - examples of requirements text for at least some of the clauses.

OVERWIEV
OF SC 27 PROGRAMME OF WORK BY WORKING GROUPS

SC 27/WG 1 Mission

Information Security Management Systems

The scope covers all aspects of standardisation related to information security management systems:

a) Management system requirements;

b) ISMS methods and processes, implementation guidance, codes of practice for information security controls;

c) Sector and application specific use of ISMS;

d) Accreditation, certification, auditing of ISMS;

e) Competence requirements for information security management system professionals

f) Governance;

g) Information security economics.

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27000	Overview and vocabulary	5th ed. 2018	*This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.*
ISO/IEC 27001	Information security management systems – Requirements	2nd ed. 2013	*This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's business activities and the risks it faces.*
ISO/IEC 27002	Code of practice for information security controls	2nd ed. 2013 *(revision WD3)*	*This International Standard offers a collection of commonly accepted information security control objectives and controls and includes guidelines for implementing these controls.*
ISO/IEC 27003	Information security management system - guidance	2nd ed. 2017	*This International Standard provides further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review and improve the ISMS.*
ISO/IEC 27004	Information security management Monitoring, measurement, analysis and evaluation	2nd ed. 2016	*This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems.*

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27005	Information security risk management	3rd ed. 2018 (revision WD)	*This International Standard provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.*
ISO/IEC 27006	International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems	3rd ed. 2016 (DAMD1)	*This International Standard specifies general requirements for a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration. This International Standard follows the structure of ISO/IEC 17021 with the inclusion of additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification.*
ISO/IEC 27007	Guidelines for information security management systems auditing	2nd ed. 2017 *(under revision DIS)*	*This International Standard provides guidance on conducting information security management system (ISMS) audits, as well as guidance on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. It is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.*
ISO/IEC TR 27008	Guidelines for auditors on ISMS controls	2nd ed. 2019	*This Technical Report provides guidance for assessing the implementation of ISMS controls selected through a risk-based approach for information security management. It supports the information security risk management process and assessment of ISMS controls by explaining the relationship between the ISMS and its supporting controls.*

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements	1st ed. 2016 (revision DIS)	*This International Standard defines the requirements for the use of ISO/IEC 27001 for sector-specific applications. It explains how to include requirements additional to those in ISO/IEC 27001. This International Standard also explains how to include controls or control sets in addition to ISO/IEC 27001 Annex A. This International Standard also specifies principles on the refinement of ISO/IEC 27001 requirements. This International Standard prohibits requirements which are in conflict with ISO/IEC 27001 requirements.*
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications	2nd ed. 2015	*This International Standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-sector communications.*
ITU-T X.1051 | ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	2nd ed. 2016 (revision proposed)	*This Recommendation | International Standard: a) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications organizations based on ISO/IEC 27002; b) provides an implementation baseline of Information Security Management within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities and services.*

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	2nd ed. 2015 (revision WD)	*This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations which are intending to either: a. Implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa; b. Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or c. Align existing ISO/IEC 27001 and ISO/IEC 20000-1 management system (MS) implementations.*
ITU-T X.1054 | ISO/IEC 27014	Governance of information security	1st ed. 2013 (revision CD)	*This International Standard provides guidance on the development and use of governance of information security (GIS) through which organisations direct and control the information security management system (ISMS) process as specified in ISO/IEC 27001. This International Standard provides guiding principles and processes for top management of organisations on the effective, efficient, and acceptable use of information security within their organisations.*
ISO/IEC TR 27016	Information security management - Organisational economics	1st ed. 2013	*This Technical Report provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources.*
ITU-T X.1631 | ISO/IEC 27017	Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	1st ed. 2015	*This Technical Specification/ International Standard is to define guidelines supporting the implementation of Information Security Management for the use of cloud service. The adoption of this Technical Specification/ International Standard allows cloud consumers and providers to meet baseline information security management with the selection of appropriate controls and implementation guidance based on risk assessment for the use of cloud service.*

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	2nd edition 2017 (corrected 2019-08)	*This Technical Report provides guidance for process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes.*
ISO/IEC 27021	Competence Requirements for information security Management Professionals	*1st edition 2017*	*This document specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving an information security management system that to ISO/IEC 27001.*
ISO/IEC 27022	Guidance on ISMS processes	*WD2*	*This document provides a process reference model (PRM) for information security management, which clearly differentiates between ISMS processes and measures/controls. A PRM is a model comprising definitions of processes described in terms of process purpose and outputs, together with an architecture describing the relationships between the processes. Using the PRM in a practical application may require additional elements suited to the environment and circumstances.* *The PRM specified in this document describes the ISMS processes implied by ISO/IEC 27001. The PRM is intended to be used as a process implementation and operation guide.*

WG 1 Products

Standard	Title	Status	Abstract
ISO/IEC 27100	Cybersecurity – Overview and concepts	*WD2*	This document provides the overview of cybersecurity. The terms and definitions provided in this document — describe cybersecurity and relevant concepts do not cover all terms and definitions applicable to cybersecurity; and do not limit other standards in defining new cybersecurity- related terms for use.
ISO/IEC 27101	Cybersecurity Framework development guidelines	*WD3*	This document specifies guidelines for developing a cybersecurity framework. This document is applicable to cybersecurity framework creators in organizations regardless of their type, size, or nature.
ISO/IEC 27102	Guidelines for cyber insurance	*1st ed. 2019*	This document gives guidelines for: (a) The use of insurance as a form of risk transfer to help an organization manage the impact of cybersecurity incidents; (b) Sharing data and information between an insurer and insured party to prepare, negotiate, accept, monitor and deal with claims associated with a cyber insurance policy; (c) Assisting information security professionals use cyber insurance for risk treatment; (d) How an ISMS can contribute to communicating and demonstrating cyber insurability
ISO/IEC TR 27103	Cyber security and ISO and IEC standards	*1st. ed. 2018*	This TR demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.

WG 1 Standing Documents

SD	Title
SD 2	Guidance Terminology Process
SD 7	Use of ISO/IEC family of standards in Governmental / Regulatory requirements
SD 8	Use Case Examples for the Application of ISO/IEC 27009

SC 27/WG 2 Mission

- Cryptography and Security Mechanisms
- The Terms of Reference:
  - *Identify the need and requirements for these techniques and mechanisms in IT systems and applications; and*
  - *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.*

WG 2 Products

Standard	Title	Status	Abstract
ISO/IEC 18033-1	Encryption algorithms Part 1: General	1st ed. 2005 under revision	ISO/IEC 18033 specifies asymmetric ciphers (including identity-based ciphers, homomorphic encryption) and symmetric ciphers (block ciphers and stream ciphers).
-2	Part 2: Asymmetric ciphers	1st ed. 2006 (+Amd 1)	
-3	Part 3: Block ciphers	2nd ed. 2010	
-4	Part 4: Stream ciphers	2nd ed. 2011	
-5	Part 5: Identity-based ciphers	1st ed. 2015	
-6	Part 6: Homomorphic encryption	1st ed. 2019	
ISO/IEC 29192-1	Lightweight cryptography Part 1: General	1st ed. 2012	ISO/IEC 29192 specifies symmetric ciphers (block ciphers and stream ciphers) , mechanisms using asymmetric techniques (authentication, key exchange and identity-based signature), hash functions, message authentication codes (MACs) and broadcast authentication protocols which are suitable for lightweight cryptographic applications.
-2	Part 2: Block ciphers	1st ed. 2012	
-3	Part 3: Stream ciphers	1st ed. 2012	
-4	Part 4: Mechanisms using asymmetric techniques	1st ed. 2013	
-5	Part 5: Hash-functions	1st ed. 2016	
-6	Part 6: Message authentication codes (MACs)	*1st ed. 2019*	
-7	Part 7: Broadcast authentication protocols	1st ed. 2019	
-8	Part 8: Authenticated encryption	under development	

WG2 Products

Standard	Title	Status	Abstract
ISO/IEC 29150	Signcryption	1st ed. 2011	ISO/IEC 29150 specifies mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to their own public and private key pairs.
ISO/IEC 19772	Authenticated encryption	1st ed. 2009	ISO/IEC 19772 specifies methods for authenticated encryption, i.e., defined ways of processing a data string for data confidentiality, data integrity and data origin authentication.
ISO/IEC 10116	Modes of operation for an n-bit block cipher algorithm	4th ed. 2017	ISO/IEC 10116 specifies modes of operation for a block cipher algorithm, i.e., ECB, CBC, OFB, CFB and CTR.
ISO/IEC 10118-1	Hash-functions Part 1: General	3rd ed. 2016	ISO/IEC 10118 specifies some kinds of hash-functions which map arbitrary strings of bits to a given range.
-2	Part 2: Hash-functions using an n-bit block cipher	3rd ed. 2010	
-3	Part 3: Dedicated hash-functions	4th ed. 2018	
-4	Part 4: Hash-functions using modular arithmetic	1st ed. 1998	
ISO/IEC 15946-1	Cryptographic techniques based on elliptic curves Part 1: General	3rd ed. 2016	ISO/IEC 15946 describes the mathematical background and general techniques in addition to the elliptic curve generation techniques.
-5	Part 5: Elliptic curve generation	2nd ed. 2017	

WG 2 Products

Standard	Title	Status	Abstract
ISO/IEC 9796-2	Digital signature schemes giving message recovery Part 2: Integer factorization based mechanisms	3rd ed. 2010	ISO/IEC 9796-2 specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead.
-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006	
ISO/IEC 14888-1	Digital signatures with appendix Part 1: General	2nd ed. 2008	ISO/IEC 14888 specifies digital signature mechanisms with appendix.
-2	Part 2: Integer factorization based mechanisms	2nd ed. 2008	
-3	Part 3: Discrete logarithm based mechanisms	4th ed. 2018	
ISO/IEC 20008-1	Anonymous digital signatures Part 1: General	1st ed. 2013	ISO/IEC 20008 specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.
-2	Part 2: Mechanisms using a group public key	1st ed. 2013	
-3	Part 3: Mechanisms using multiple public keys	under development	
ISO/IEC 18370-1	Blind digital signatures Part 1: General	1st ed. 2016	ISO/IEC 18370 specifies blind digital signature mechanisms which allow a recipient to obtain a signature without giving signer any information about the actual message or resulting signature.
-2	Part 2: Discrete logarithm based mechanisms	1st ed. 2016	
ISO/IEC 23264-1	Redaction of authentic data Part 1: General	under development	ISO/IEC 23264 specifies cryptographic mechanisms to redact authentic data and their properties. This standard also contains definitions and symbols. In particular, it defines the processes involved in those mechanisms, the participating parties, and the cryptographic properties.
-2	Part 2: Redactable signature schemes based on asymmetric mechanisms	under development	

WG2 Products

Standard	Title	Status	Abstract
ISO/IEC 9798-1	Entity authentication Part 1: General	3rd ed. 2010	ISO/IEC 9798 specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret.
-2	Part 2: Mechanisms using symmetric encipherment algorithms	4th ed. 2019	
-3	Part 3: Mechanisms using digital signature techniques	3rd ed. 2019	
-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009 under revision	
-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	
ISO/IEC 20009-1	Anonymous entity authentication Part 1: General	1st ed. 2013	ISO/IEC 20009 specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity, and which based on blind signatures and weak secrets.
-2	Part 2: Mechanisms based on signatures using a group public key	1st ed. 2013	
-3	Part 3: Mechanisms based on blind signatures	under development	
-4	Part 4: Mechanisms based on weak secrets	1st ed. 2017	

WG2 Products

Standard	Title	Status	Abstract
ISO/IEC 9797-1	Message authentication codes (MACs) Part 1: Mechanisms using a block cipher	2nd ed. 2011	ISO/IEC 9797 specifies message authentication code (MAC) algorithms, which are data integrity mechanisms that compute a short string.
-2	Part 2: Mechanisms using a dedicated hash-function	2nd ed. 2011 under revision	
-3	Part 3: Mechanisms using a universal hash-function	1st ed. 2011	
ISO/IEC 7064	Check character systems	1st ed. 2003	ISO/IEC 7064 specifies a set of check character systems capable of protecting strings against errors.
ISO/IEC 11770-1	Key management Part 1: Framework	2nd ed. 2010	ISO/IEC 11770 describes general models on which key management mechanisms are based, defines the basic concepts of key management, and defines several kinds of key establishment mechanisms .
-2	Part 2: Mechanisms using symmetric techniques	3rd ed. 2018	
-3	Part 3: Mechanisms using asymmetric techniques	3rd ed. 2008 (+Amd 1)	
-4	Part 4: Mechanisms based on weak secrets	2nd ed. 2017	
-5	Part 5: Group key management	1st ed. 2011 under revision	
-6	Part 6: Key derivation	1st ed. 2016	
-7	Part 7: Cross-domain password-based authenticated key exchange	under development	

WG2 Products

Standard	Title	Status	Abstract
ISO/IEC 13888-1	Non-repudiation Part 1: General	3rd ed. 2009 under revision	ISO/IEC 13888 specifies for the provision of non-repudiation services. The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action to resolve disputes about the occurrence or non-occurrence of the event or action. The event or act on can be the generation, sending, receipt, submission, or transport of a message.
-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2010	
-3	Part 3: Mechanisms using asymmetric techniques	2nd ed. 2009 under revision	
ISO/IEC 18014-1	Time-stamping services Part 1: Framework	2nd ed. 2008	ISO/IEC 18014 defines time-stamping services that are provided using time-stamp tokens between the participating entities in addition to the traceability of time sources.
-2	Part 2: Mechanisms producing independent tokens	2nd ed. 2009 under revision	
-3	Part 3: Mechanisms producing linked tokens	2nd ed. 2009	
-4	Part 4: Traceability of time sources	1st ed. 2015	
ISO/IEC 18031	Random bit generation	2nd ed. 2011 (+Amd1)	ISO/IEC 18031 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model.
ISO/IEC 18032	Prime number generation	1st ed. 2005 under revision	ISO/IEC 18032 presents methods for generating prime numbers as required in cryptographic protocols and algorithms.
ISO/IEC 19592-1	Secret sharing Part 1: General	1st ed. 2016	ISO/IEC 19592 describes cryptographic secret sharing schemes and their properties.
-2	Part 2: Fundamental mechanisms	1st ed. 2017	

(SC 27 WELCOME PACKAGE 2019-09)

WG2 Future Considerations

Topics	Status
Suitability of standardization of format-preserving encryption schemes in ISO/IEC standards	Study Period
Elliptic curve generation	Study Period
Password-based key derivation	Study Period
ISO/IEC 20008-3: Mechanisms using multiple public keys	Study Period
Suitability of Inclusion of Deoxys-TBC in ISO/IEC 18033-3	Study Period
Suitability of Inclusion of Skinny in ISO/IEC 18033-3	Study Period
Security of Mechanism 6 of ISO/IEC 20008-2	Study Period
Stateful hash-based signatures	Study Period
New results concerning Streebog and Kuznyechik S-box	Study Period
Inclusion of secret sharing related technologies	Study Period

SC 27/WG 3 Mission

Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

a) security evaluation criteria;

b) methodology for application of the criteria;

c) security functional and assurance specification of IT systems, components and products;

d) testing methodology for determination of security functional and assurance conformance;

e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

WG 3 Standards

Standard	Title	Status	Abstract
ISO/IEC 15408	Evaluation criteria for IT security	3rd ed. 2009 under revision CD stage	ISO/IEC 15408 establishes the security evaluation criteria and concepts to provide a general model of evaluation of the security properties of IT products. The current draft structure of the standard includes the following parts: • Introduction and general model • Security functional components • Security assurance components • Framework for the specification of evaluation methods and activities • Pre-defined packages of security requirements
ISO/IEC TR 15443	A framework for IT security assurance	3rd ed. 2012	The objective of this Technical Report is to present a variety of assurance methods and assurance approaches to guide the IT Security Professional in the selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given IT security product, system, service, process or environmental factor satisfies its stated security assurance requirements.
ISO/IEC TR 15446	Guide for the preparation of Security Targets and Protection Profiles	3rd ed. 2017 2nd ed. 2009 1st ed. 2004	Many people consider this Technical Report to be a very good introduction to ISO/IEC 15408. It also provides practical guidance to the process of preparing for evaluation.
ISO/IEC 17825	Non-invasive attack mitigation test metrics for cryptographic modules	1st ed. 2016	ISO/IEC 17825 is applicable to all parties involved in designing and testing cryptographic modules or similar security devices. It provides the methods and metrics for testing of mitigation for classes of non-invasive security attacks.
ISO/IEC 18045	Methodology for IT security evaluation	2nd ed. 2008 under revision CD stage	ISO/IEC 18045 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.
ISO/IEC 18367	Cryptographic algorithms and security mechanisms conformance testing	1st ed. 2016	ISO/IEC 18367 describes cryptographic algorithms and security mechanisms conformance testing methods.

Standard	Title	Status	Abstract
ISO/IEC TS 19249	Catalogue of architectural and design principles for secure products, systems, and applications	1st ed. 2017	ISO/IEC TS 19249 provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively.
ISO/IEC TS 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	1st ed. 2018	ISO/IEC 29100 defines a framework of privacy principles that should be considered when developing systems or applications that deal with personally identifiable information.
ISO/IEC 19790	Security requirements for cryptographic modules	2nd ed. 2012 corrected 2015 1st e. 20006 Cor 1:2015	ISO/IEC 19790 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems
ISO/IEC TR 19791	Security Assessment of Operational Systems	2nd ed. 2010	ISO/IEC TR 19791 provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408 by considering a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation
ISO/IEC 19792	A Framework for security evaluation and testing of biometric technology	1st ed. 2009	ISO/IEC 19792 specifies the subjects to be addressed during a security evaluation of a biometric system. It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system.
ISO/IEC 19896	Competence requirements for information security testers and evaluators	1st ed. 2018	ISO/IEC 19896 provides the minimum requirements for the knowledge, skills and effectiveness requirements of individuals performing testing activities for a conformance scheme using ISO/IEC 19790 and of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045.
ISO/IEC 19989	Criteria and methodology for security evaluation of biometric systems	under development CD stage	For the security evaluation of presentation attack detection for biometrics, this International Standard will specify extended functional security functional components to ISO/IEC 15408-2, extended security assurance components to ISO/IEC 15408-3, and will complement the methodology specified in ISO/IEC 18045.

Standard	Title	Status	Abstract
ISO/IEC TR 20004	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	2nd ed. 2015	ISO/IEC TR 20004 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.
ISO/IEC 20085	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules	under development Pending publication	The document will address the specific tools, test bench setups, data capture and the determination of the pass/fail metric based on the collected data. The calibration of the tools, setup, etc. will also be addressed to ensure that test setups that may have different underlying components yield the same results.
ISO/IEC TS 20540	Testing cryptographic modules in their operational environment	1st ed. 2018	ISO/IEC TS 20540 provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.
ISO/IEC 20543	Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408	1st ed. 2019	This project aims to specify a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications.
ISO/IEC 20897	Security requirements and test methods for physically unclonable functions for generating non-stored security parameters	under development DIS stage	This project will specify the security requirements and the test methods for physically unclonable functions for generating non-stored cryptographic parameters.
ISO/IEC TR 21827	Introductory guidance on evaluation for IT security	2nd ed. 2008	This Technical Report will provide guidance and support to those responsible for implementing the revised edition of the ISO/IEC 15408 and ISO/IEC 18045 standards.
ISO/IEC TR 22216	Introductory guidance on evaluation for IT security	under development WD stage	This Technical Report will provide guidance and support to those responsible for implementing the fourth edition of the ISO/IEC 15408 and ISO/IEC 18045 standards. This edition of the ISO/IEC 15408 and ISO/IEC 18045 standards includes substantial changes from the third edition.

Standard	Title	Status	Abstract
ISO/IEC TS 23532	Requirements for the competence of IT security testing and evaluation laboratories	under development WD stage	This proposed new technical specification will supplement the CASCO standard ISO/IEC 17025 by providing more detail and specificity to the requirements of ISO/IEC 17025 in the specialised area for laboratories performing evaluations and testing based on the ISO/IEC 15408 and ISO/IEC 19790 standards.
ISO/IEC 23837	Security requirements, test and evaluation methods for quantum key distribution	under development WD stage	The proposed International Standard specifies the security requirements, test and evaluation methods for Quantum Key Distribution (QKD).
ISO/IEC 24759	Test requirements for cryptographic modules	2nd ed. 2017	ISO/IEC 24759 specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790.
ISO/IEC 29128	Verification of cryptographic protocols	1st ed. 2014 under revision WD stage	ISO/IEC 29128 provides a technical base for the assessment of the security of cryptographic protocols.
ISO/IEC 29147	Responsible Vulnerability Disclosure	2nd ed. 2018	ISO/IEC 29147 provides a methodology for the disclosure and management of vulnerability alerts to be used by all interested parties.
ISO/IEC TS 30104	Physical security attacks, mitigation techniques and security requirements	1st ed. 2015	ISO/IEC TS 30104 provides a survey of physical security attacks directed against different types of hardware embodiments; guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks.
ISO/IEC 30111	Vulnerability handling processes	2nd ed. 2019 1st ed. 2013	ISO/IEC 30111 gives guidelines for how to process and resolve potential vulnerability information reported by individuals or organisations that find a potential vulnerability.

WG3 Future Considerations

Topic	Status
Evaluation criteria for connected vehicle information security based on ISO/IEC 15408	Study Period
The concept hierarchy for terminology used in SC27/WG 3 projects in particular focused on the ISO/IEC 15408 and ISO/IEC 18045 projects	Study Period

SC 27/WG 4 Mission

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.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27031	Information technology – Security techniques – Guidelines for ICT readiness for business continuity	1st ed. 2011	Describes the concepts and principles of ICT readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects for improving an organization's ICT readiness to ensure business continuity.
ISO/IEC 27031 (under revision)	Information technology – Cybersecurity – Information and communication technology readiness for business continuity	6th WD	Describes the concepts and principles of ICT readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects for improving an organization's ICT readiness to ensure business continuity.
ISO/IEC 27037	Guidelines for the identification, collection, acquisition and preservation of digital evidence	1st ed. 2012	Provides guidelines for specific activities in the handling of digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.
ISO/IEC 27039	Information technology – Security techniques – Selection, deployment and operation of intrusion detection and prevention systems (IDPS)	1st ed. 2015 Cor. 1 2016	Provides guidelines to assist organizations in preparing to deploy Intrusion Detection Prevention System (IDPS). In particular, it addresses the selection, deployment and operations of IDPS. It also provides background information from which these guidelines are derived.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27035	Information technology – Security techniques – Information security incident management	1st ed. 2011 (Withdrawn) *Revised by ISO/IEC 27035-1:2016*	Provides a structured and planned approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management.
ISO/IEC 27035-1 (under early revision)	Information technology – Information security incident management – Part 1: Principles of incident management	1st ed. 2016	Presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.
ISO/IEC 27035-2 (under early revision)	Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response	1st ed. 2016	Provides the guidelines to plan and prepare for incident response. The guidelines are based on the "Plan and Prepare" phase and the "Lessons Learned" phase of the "Information security incident management phases" model presented in Part 1.
ISO/IEC 27035-3	Information technology – Information security incident management – Part 3: Guidelines for incident response operations	2nd WD	Includes staff responsibilities and operational incident response activities across the organization. Particular focus is given to the incident response team activities including monitoring, detection, analysis, and response activities for the collected data or security events.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27041	Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method	1st ed. 2015	Provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are “fit for purpose”.
ISO/IEC 27042	Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence	1st ed. 2015	Provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility and repeatability.
ISO/IEC 27043	Information technology -- Security techniques -- Incident investigation principles and processes	1st ed. 2015	Provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27050-1	Information technology -- Security techniques -- Electronic discovery -- Part 1: Overview and concepts	1st ed. 2016	Provides an overview of electronic discovery. In addition, it defines related definitions and describes the concepts, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI).
ISO/IEC 27050-2	Information technology -- Electronic discovery -- Part 2: Guidance for governance and management of electronic discovery	1st ed. 2018	Provides guidance for technical and non-technical personnel at senior levels within an organization, including those with responsibility for compliance with regulatory requirements, industry standards and, in some jurisdictions, legal requirements.
ISO/IEC 27050-3	Information technology -- Security techniques -- Electronic discovery -- Part 3: Code of practice for electronic discovery	1st ed. 2017	Provides requirements and guidance on activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI)
ISO/IEC 27050-4	Information technology – Electronic discovery – Part 4: Technical readiness	1st CD	Provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes.

WG 4 Products

Standard	Title	Status	Abstract
ISO/IEC 27033-1	Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts	2nd ed. 2015	Provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security.
ISO/IEC 27033-2	Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security	1st ed. 2012 Confirmed in 2018	Provides guidelines for organizations to plan, design, implement and document network security.
ISO/IEC 27033-3	Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues	1st ed. 2010 Confirmed in 2013	Describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks.
ISO/IEC 27033-4	Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways	1st ed. 2014	Gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways
ISO/IEC 27033-5	Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	1st ed. 2013	Gives guidelines for the selection, implementation and monitoring of the technical controls necessary to provide network security using Virtual Privates Network (VPN) connections to inter-connect networks and connect remote users to networks.
ISO/IEC 27033-6	Information technology -- Security techniques -- Network security -- Part 6: Securing wireless IP network access	1st ed. 2016	Describes the threats, security requirements, security control and design techniques associated with wireless networks. It provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless network.

WG 4 Products

Standard	Title	Status	Abstract
ISO/IEC 27036-1	Information technology -- Security techniques -- Information security for supplier relationships – Part 1: Overview and concepts	1st ed. 2014 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It addresses perspectives of both acquirers and suppliers.
ISO/IEC 27036-2	Information technology -- Security techniques -- Information security for supplier relationships – Part 2: Requirements	1st ed. 2014	Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.
ISO/IEC 27036-3	Information technology -- Security techniques -- Information security for supplier relationships – Part 3: Guidelines for ICT supply chain security	1st ed. 2013	Provides product and service acquirers and suppliers in ICT supply chain with guidance.
ISO/IEC 27036-4	Information technology -- Security techniques -- Information security for supplier relationships – Part 4: Guidelines for security of cloud services	1st ed. 2016	Define guidelines supporting the implementation of Information Security Management for the use of cloud service.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27038	Information technology -- Security techniques -- Specification for digital redaction	1st ed. 2014	Specifies characteristics of techniques for performing digital redaction on digital documents. It also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed.
ISO/IEC 27040	Information technology -- Security techniques -- Storage security	1st ed. 2015	Provides detailed technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security.
ISO/IEC 27045	Information technology – Big data security and privacy – Processes	2nd WD	Defines process reference, assessment and maturity models for the domain of big data security and privacy. These models are focused on process architecture and the processes used to achieve big data security and privacy, most specifically on the maturity of those processes.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27034-1	Information technology – Application security – Part 1: Overview and concepts	1st ed. 2011 Cor. 1 2014 Confirmed in 2017	Provides guidance to assist organizations in integrating security into the processes used for managing their applications. This International Standard presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.
ISO/IEC 27034-2	Information technology – Application security – Part 2: Organization normative framework	1st ed. 2015	Provides a detailed description of the Organization Normative Framework and provides guidance to organizations for its implementation.
ISO/IEC 27034-3	Information technology – Application security – Part 3: Application security management process	1st ed. 2018	Provides a detailed description and implementation guidance for the Application Security Management Process.
ISO/IEC 27034-4	Information technology – Application security – Part 4: Validation and verification	5th CD	Provides a detailed description of an Application security validation process used to audit and verify Application Security.
ISO/IEC 27034-5	Information technology – Application security – Part 5: Protocols and application security control data structure	1st ed. 2017	Outlines and explains the minimal set of essential attributes of Application Security Controls (ASCs) and details the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM).

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC TS 27034-5-1	Information technology – Application security – Part 5-1: Protocols and application security control data structure – XML Schemas	1st ed. 2018	Defines XML Schemas that implement the minimal set of information requirements and essential attributes of Application Security Controls (ASCs) and the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM) from Part 5.
ISO/IEC 27034-6	Information technology – Application security – Part 6: Case studies	1st ed. 2016	Provides usage examples of Application Security Controls (ASCs) for specific applications.
ISO/IEC 27034-7	Information technology – Application security – Part 7: Assurance prediction framework	1st ed. 2018	Provides the criteria and guidance for the extension of security attributes in one application to a different but related application. Additionally the prediction will state the conditions under which the prediction is valid and invalid.

SC 27 WG 5 Mission

Identity Management & Privacy Technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - *Identity management*
  - *Biometrics, and*
  - *Privacy*

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 24761	Authentication context for biometrics	1st ed. 2009 Cor.1: 2013-03-01 under revision (FDIS)	ISO/IEC 24761 specifies the structure and the data elements of Authentication Context for Biometrics (ACBio) used for checking the validity of the result of a biometric verification process executed at a remote site. It allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. ISO/IEC 24761 also specifies the cryptographic syntax of an ACBio instance based on an abstract Cryptographic Message Syntax (CMS) schema.
ISO/IEC 24745	Biometric information protection	1st ed. 2011 under revision (WD)	ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.
ITU-T X.1085 | ISO/IEC 17922	Telebiometric authentication framework using biometric hardware security module	1st ed. 2017	ITU-T X.1085 | ISO/IEC 17922 describes a telebiometric authentication scheme using a biometric hardware security module (BHSM) for the telebiometric authentication of the person who presents the BHSM as the owner of an ITU-T X.509 certificate embedded in the BHSM as registered with the Certification Authority (CA). It provides the requirements for deploying a BHSM scheme to provide secure telebiometric authentication within PKI environments. The scheme provides assurance for telebiometric authentication using biometric recognition integrated into a hardware security module. It also provides ASN.1 definitions that allow the biometric authentication to be incorporated into an ITU-T X.509 framework to authenticate the user as the owner of the ITU-T X.509 certificate.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 24760-1	A framework for identity management – Part 1: Terminology and concepts	2nd ed. 2019 1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	ISO/IEC 24760-1 • defines terms for identity management, and • specifies core concepts of identity and identity management and their relationships. To address the need to efficiently and effectively implement systems that make identity-based decisions ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations. ISO/IEC 24760-1 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations. ISO/IEC 24760-1 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.
ISO/IEC 24760-2	A framework for identity management – Part 2: Reference architecture and requirements	1st ed. 2015	ISO/IEC 24760-2 • provides guidelines for the implementation of systems for the management of identity information, and • specifies requirements for the implementation and operation of a framework for identity management. ISO/IEC 24760-2 is applicable to any information system where information relating to identity is processed or stored.
ISO/IEC 24760-3	A framework for identity management – Part 3: Practice	1st ed. 2016	ISO/IEC 24760-3 provides practices for identity management, e.g. for assurance in identity information use, and controlling the access to identity information.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 29100	Privacy framework	1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html Amendment published 2018-06	ISO/IEC 29100 provides a privacy framework which • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for IT. ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.
ISO/IEC 29191	Requirements for partially anonymous, partially unlinkable authentication	1st ed. 2012	ISO/IEC 29191 provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication. The term 'partially anonymous, partially unlinkable' means that an a priori designated opener, and that designated opener only, can identify the authenticated entity.
ISO/IEC 29101	Privacy architecture framework	2nd ed. 2018 1st ed. 2013	ISO/IEC 29101 defines a privacy architecture framework that: • specifies concerns for ICT systems that process PII; • lists components for the implementation of such systems; and • provides architectural views contextualizing these components. This document is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII. It focuses primarily on ICT systems that are designed to interact with PII principals.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 29115	Entity authentication assurance framework	1st ed. 2013 under revision (WD)	ISO/IEC 29115 provides a framework for managing entity authentication assurance in a given context. In particular, it: • specifies 4 levels of entity authentication assurance (LoA); • specifies criteria and guidelines for achieving these 4 levels; • provides guidance for mapping other authentication assurance schemes to the 4 LoAs and for exchanging the results of authentication that are based on the 4 LoAs; and • provides guidance on mitigating authentication threats.
ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors	1st ed. 2014 2nd ed. 2019	ISO/IEC 27018 establishes control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, ISO/IEC 27018 specifies guidelines based on ISO/IEC 27002, considering the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services. The guidelines in ISO/IEC 27018 might also be relevant to organizations acting as PII controllers; however, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. ISO/IEC 27018 is not intended to cover such additional obligations.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 29190	Privacy capability assessment model	1st ed. 2015	ISO/IEC 29190 provides organizations with guidance how to assess their capability to manage privacy-related processes. In particular, it: (i) specifies steps in assessing processes to determine privacy capability; (ii) specifies a set of levels for privacy capability assessment; iii) provides guidance on the key process areas against which privacy capability can be assessed; (iv) provides guidance for those implementing process assessment; and (v) provides guidance on how to integrate the privacy capability assessment into organizations operations.
ISO/IEC 29146	A framework for access management	1st ed. 2016	ISO/IEC 29146 defines and establishes a framework for access management (AM) and the secure management of the process to access information and Information and Communications Technologies (ICT) resources, associated with the accountability of a subject within some context.
ISO/IEC 29134	Guidelines for privacy impact assessment	1st ed. 2017	ISO/IEC 29134:2017 gives guidelines for - a process on privacy impact assessments (PIAs), and - a structure and content of a PIA report. It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations. ISO/IEC 29134:2017 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

WG 5 Products

Standard	Title	Status	Abstract
ITU-T X.gpim | ISO/IEC 29151	Code of practice for personally identifiable information protection	1st ed. 2017	ISO/IEC 29151:2017 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). In particular, it specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s). It is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.
ISO/IEC TS 29003	Identity proofing	1st ed. 2018	ISO/IEC TS 29003:2018 - gives guidelines for the identity proofing of a person; - specifies levels of identity proofing, and requirements to achieve these levels - is applicable to identity management systems
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	1st ed. 2018	ISO/IEC 20889:2018 provides a description of privacy-enhancing data de-identification techniques to describe and design de-identification measures in accordance with the privacy principles in ISO/IEC 29100. In particular, it specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification. It is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, that are PII controllers or PII processors implementing data de-identification processes for privacy enhancing purposes.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC TR 27550	Privacy engineering for system life cycle processes	1st ed. 2019	ISO/IEC 27 provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes: • it describes the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and • it describes privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design. The intended audience includes engineers and practitioners who are involved in the development, implementation or operation of systems that need privacy consideration, as well as managers in organizations responsible for privacy, development, product management, marketing, and operations.
ISO/IEC 27701	Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines	1st ed. 2019	ISO/IEC 27701 specifies the requirements for establishing, implementing, maintaining and continually improving a privacy-specific information security management system. a management system for protecting personal data. Formerly referred to as ISO/IEC 27552, it builds on ISO/IEC 27001, Information Technology – Security techniques – Information security management systems – Requirements providing the necessary extra requirements when it comes to privacy.

WG 5 Products

Project	Title	Status
Standing Document 1	WG 5 Roadmap	
Standing Document 2	Privacy references list	Freely available via www.jtc1sc27.din.de/en
Standing Document 4	Standards privacy assessment	Freely available via www.jtc1sc27.din.de/en

WG 5 Projects

Project	Title	Status
ISO/IEC 29184	Online privacy notices and consent	DIS
ISO/IEC 27550	Privacy engineering for system life cycle processes	under publication
ISO/IEC 27552	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines	under publication
ISO/IEC 27551	Requirements for attribute-based unlinkable entity authentication	CD
ISO/IEC 27553	Security requirements for authentication using biometrics on mobile devices	WD
ISO/IEC 27554	Application of ISO 31000 for assessment of identity management-related risk	WD
ISO/IEC 27555	Establishing a PII deletion concept in organizations	WD
ISO/IEC 27556	User-centric framework for the handling of Personal Identifiable Information (PII) based on privacy preferences	WD
Study Period	Privacy consideration in practical workflows	Continuing
Study Period	Additional privacy-enhancing data de-identification standards	Continuing
Study Period	Identity standards landscape document update	Continuing
Study Period	Impact of artificial intelligence on privacy	Continuing
Study Period	Use cases for identity assurance	Continuing
Study Period	Consent receipts and records	Starting
Study Period	Privacy engineering model	Starting
Study Period	Review of requirements for accredited certification for ISO/IEC 27552 implementations	Starting

Contact Point

For further information contact
the ISO/IEC JTC 1/SC 27 Committee Manager:

krystyna.passia@din.de