ISO/IEC JTC 1/SC 27 N17600

REPLACES: N16401

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	**officers' contribution**
TITLE:	**ISO/IEC JTC 1/SC 27 Corporate Presentation**
SOURCE:	**JTC 1/SC 27**
DATE:	**2017-07-18**
PROJECT:	
STATUS:	**This document is circulated for information.**
PLEASE NOTE:	**This document is also publicly accessible from the public website of SC 27 at: http://www.din.de/go/jtc1sc27**
ACTION ID:	**FYI**
DUE DATE:	
DISTRIBUTION:	**P-, L-, O-Members** **W. Fumy, SC 27 Chairman** **M. De Soete, 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 + 56**

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e. V., Am DIN-Platz, Burggrafenstr. 6, D-10787 (postal D-10772) Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-4-2652; E-mail: krystyna.passia@din.de;
HTTP://www.din.de/go/jtc1sc27

Corporate Presentation

ISO/IEC JTC 1/SC 27

IT Security Techniques

(ver 19/July 2017)

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

SC27 Mission

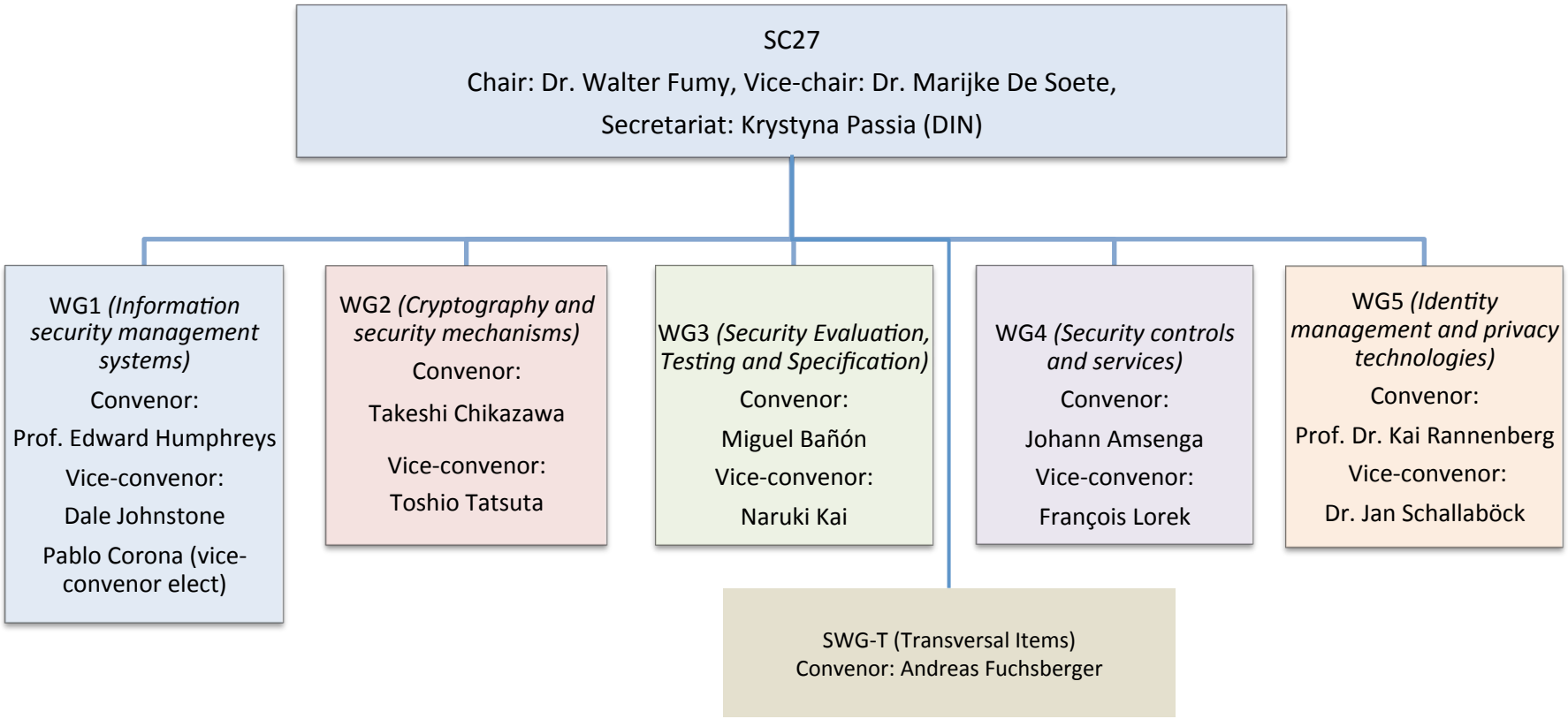
The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management 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.

(go to http://www.din.de/en/meta/jtc1sc27)

SC27 Structure



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)*

Projects Facts & Figures

- Projects
  - Total no of projects: 250
  - No of active projects: 85
  - Current number of published standards: 164
- 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)

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.*

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.

SC27 Members

P-members (voting)

Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Côte-d'Ivoire, Cyprus, Czech Republic, Denmark, Finland, France, Germany, India, Indonesia, Ireland, Italy, Israel, Jamaica, Japan, Kazakhstan, Kenya, Rep. of Korea, Lebanon, Luxembourg, Rep. of Macedonia, Malaysia, Mauritius, Mexico, The Netherlands, New Zealand, Norway, Panama, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, Rwanda, Singapore, Slovakia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay (Total: 55)

O-members (observing)

Belarus, Bosnia and Herzegovina, Bulgaria, Costa Rica, El Salvador, Estonia, Ghana, Hong Kong, Hungary, Iceland, Islamic Rep. of Iran, Lithuania, Morocco, State of Palestine, Saudi Arabia, Serbia, Slovenia, Swaziland, Turkey (Total: 20)

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.

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.*

SC27 Liaison Partners

Internal Liaisons within ISO

- *ISO/CASCO*
- *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 1 - Quality management and quality assurance − Concepts and terminology*
- *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 262 Risk management*

SC27 Liaison Partners

Internal Liaisons within ISO

- *ISO/TC 272 Forensic sciences*
- *ISO/TC 292 Security and resilience*
- *ISO/PC 302 Revision of ISO 19011 Guidelines for auditing management systems*
- *ISO/JTCG Joint technical Coordination Group on MSS (TAG 13)*

SC27 Liaison Partners

Internal Liaisons within IEC

- *IEC/TC 45/SC 45A Instrumentation, control and electrical systems of nuclear facilities*
- *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*

SC27 Liaison Partners

Internal Liaisons within ISO/IEC JTC 1

- *JTC 1/WG 7 Sensor networks*
- *JTC 1/WG 9 Big Data*
- *JTC 1/WG 10 Internet of Things (IoT)*
- *SC 6 Telecommunications and information exchange between system*
- *SC 7 Software engineering*
- *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 31/WG 4 Automatic identification and data capture techniques*
- *SC 36 Information technology for learning, education, and training*
- *SC 37 Biometrics*
- *SC 38 Distributed application platforms and services (DAPS)*
- *SC 40 IT service management and IT governance*

SC27 Liaison Partners

External CAT A Liaisons

- *Cloud Computing Association (CSA)*
- *ECMA International*
- *European Network and Information Security Agency (ENISA)*
- *European Payment Council*
- *European Telecommunications Standards Institute (ETSI)*
- *ETSI Electronic Signature and Infrastructure*
- *ETSI Methods for Testing and Specification*
- *ETSI TC NFV - Network Functions Virtualization*
- *ETSI TC Cyber Security*
- *IEEE Computer Security*
- *Information Systems Audit and Control Association/IT Governance Institute (ISACA/ITGI)*
- *International Information Systems Security Certification Consortium, Inc. (ISC)2*

SC27 Liaison Partners

External CAT A Liaisons

- *ITU-D Study Group 2 ICT applications, cybersecurity, emergency, telecommunications and climate-change adaption*
- *ITU-T Joint coordination activity on identity management (JCA-IdM)*
- *ITU-T Focus Group on aviation applications of cloud computing for flight data monitoring (FG AC)*
- *ITU-T Study Group 13 (ITU-T SG 13): Future networks including cloud computing, mobile and next-generation networks*
- *ITU-T Study Group 15 (ITU-T SG 15): Networks, Technologies and Infrastructures for Transport, Access and Home*
- *ITU-T Study Group 17 (ITU-T SG 17): -Security*
- *MasterCard*
- *VISA Europe*

SC27 Liaison Partners

External CAT C Liaisons

- *ABC4Trust*
- *ARTICLE 29 Data Protection Working Party*
- *Common Criteria Development Board (CCDB)*
- *Cyber Security Naming and Information Structure Group Corporation*
- *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.)*
- *International Conference of Data Protection and Privacy Commissioners*
- *International Smart Card Certification Initiatives*
- *Interpol*
- *ISA99*
- *Kantara Initiative*

SC27 Liaison Partners

External CAT C Liaisons

- *OpenID Foundation*
- *Organisation for Economic Co-operation and Development (OECD)*
- *PQCrypto (Post-quantum cryptography for long term security)*
- *PRACTICE (FP7 Project: Privacy-preserving Computation in the Cloud)*
- *PRIPARE (FP7 Project)*
- *Privacy and Identity Management for Community Services (PICOS)*
- *Technology-supported Risk Estimation by Predictive Assessment of Sociotechnical Security (TREsPASS)*
- *The Open Group*
- *TM Group*
- *Trusted Computing Group (TCG)*
- *WITDOM (Empowering Privacy and Security in Non-Trusted Environments)*

SC27 Liaison Partners

External liaisons Under Vienna Agreement

- *CEN/PC 428 e-competence and IST professionalism*
- *CEN/TC 224 Personal identification, electronic signature and cards and their related systems and operations*
- *CEN/TC 377 Air Traffic Management*
- *CEN/CENELEC/ETSI/SGCG Joint CEN, CENELEC and ETSI activities on standards for Smart Grid*

SC27 WG1 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.

WG1 Products

Standard	Title	Status	Abstract
ISO/IEC 27000	Overview and vocabulary	4th ed. 2016	*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 design spec. in production)*	*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. 2016	*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.*

WG1 Products

Standard	Title	Status	Abstract
ISO/IEC 27005	Information security risk management	2nd ed. 2011 *(revision design spec. in production)*	*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	*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	1st ed. 2011 *(under revision FDIS)*	*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	1st ed. 2012 *(under revision PDTR)*	*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.*

WG1 Products

Standard	Title	Status	Abstract
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements	1st ed. 2016	*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	*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.*

WG1 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	*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 (under revision)	*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.*

WG1 Products

Standard	Title	Status	Abstract
ISO/IEC TR 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	1st ed. 2013 *(Under revision FDIS)*	*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	*Under development FDIS*	
ISO/IEC 27102	Guidelines for cyber insurance	*Under development WD*	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

WG1 Standing Documents

SD	Title
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
SD 9	Guidance Terminology Process
SD 27103 *(to be converted ISO/IEC TR 27103)*	Cyber security and ISO and IEC standards

SC27 WG2 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.*

WG2 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	
-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	Under development	
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)	Under development	
-7	Part 7: Broadcast authentication protocols	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	3rd ed. 2006 Under revision	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	3rd ed. 2006 (+Amd 1) Under revision	
-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	1st ed. 2009 Under revision	

WG2 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	3rd ed. 2016	
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	
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	

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	3rd ed. 2008 Under revision	
-3	Part 3: Mechanisms using digital signature techniques	2nd ed. 1998 (+Amd1) Under revision	
-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	Under development	

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	
-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	2nd ed. 2008 Under revision	
-3	Part 3: Mechanisms using asymmetric techniques	3rd ed. 2008	
-4	Part 4: Mechanisms based on weak secrets	1st ed. 2006 Under revision	
-5	Part 5: Group key management	1st ed. 2011	
-6	Part 6: Key derivation	1st ed. 2016	

WG2 Products

Standard	Title	Status	Abstract
ISO/IEC 13888-1	Non-repudiation Part 1: General	3rd ed. 2009	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	
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	
-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	Under development	

WG2 Future Considerations

Topics	Status
Quantum computing resistant cryptography	Study Period
Use of hash-functions in ISO/IEC 9797-2	Study Period
Redactable signatures	Study Period
Parameter choices and suitable hash-functions for ISO/IEC 29192-6 MAC algorithms	Study Period
Inclusion of LRP-AKE and RSA-AKE2 in ISO/IEC 11770-4	Study Period
Key derivation methods alignment between ISO/IEC 11770-5 and ISO/IEC 11770-6	Study Period
Revision of ISO/IEC 19772	Study Period
State of the art of symmetric key primitives and related modes of operation	Study Period
Suitable Block Cipher Block Sizes for Standardization in SC 27/WG 2	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 Products

Standard	Title	Status	Abstract
ISO/IEC 15408	Evaluation criteria for IT security	1st WD Under revision	ISO/IEC 15408:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
ISO/IEC TR 15443	A framework for IT security assurance	2nd ed.	ISO/IEC TR 15443:2012 guides the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel.
ISO/IEC TR 15446	Guide for the production of Protection Profiles and Security Targets	Revision pending publication	ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408.
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	1st ed.	ISO/IEC 17825:2016 specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4.
ISO/IEC 18045	Methodology for IT security evaluation	1st WD Under revision	ISO/IEC 18045:2008 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.

WG 3 Products

Standard	Title	Status	Abstract
ISO/IEC 18367	Cryptographic algorithms and security mechanisms conformance testing	1st ed.	ISO/IEC 18367:2016 gives guidelines for cryptographic algorithms and security mechanisms conformance testing methods.
ISO/IEC 19249	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications	Pending publication	This Technical Report (TR) provides a catalogue with guidelines for architectural and design principles for the development of secure products, systems, and applications. Applying those principles should result in more secure products, systems, and applications.
ISO/IEC 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	Pending publication	This TR provides guidance for developing privacy functional requirements as extended components based on privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2.
ISO/IEC 19790	Security requirements for cryptographic modules	2nd ed. Corrected reprint	ISO/IEC 19790:2012 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.	ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems.

WG 3 Products

Standard	Title	Status	Abstract
ISO/IEC 19792	Security evaluation of biometrics	1st Ed	ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system.
ISO/IEC 19896	Competence requirements for information security testers and evaluators	1st CD	The objective of ISO/IEC 19896 is to provide the fundamental concepts related to the topic of the competence of the individuals responsible for performing IT product evaluations and conformance testing, and to provide the specialised requirements to support competence of individuals in performing IT product evaluation and conformance testing using established standards.
ISO/IEC 19989	Criteria and methodology for security evaluation of biometric systems	2nd WD	For security evaluation of presentation attack detection for biometrics, this International Standard specifies extended security functional components, extended security assurance components, and complements to methodology specified in ISO/IEC 18045.
ISO/IEC TR 20004	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	2nd ed	SO/IEC TR 20004:2015 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008(E) 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 noninvasive attack mitigation techniques in cryptographic modules	1st CD	This standard aims at specifying what is a non-invasive attack test tool, and how to operate it. The purpose is the collection of non-invasive signals, which are attest of the security of the implementation under test (IUT).

WG 3 Products

Standard	Title	Status	Abstract
ISO/IEC TR 20540	Guidelines for testing cryptographic modules in their operational environment	1st PDTS	This Technical Report provides guidelines to audit that cryptographic module or integration of cryptographic modules is installed, configured or operated safely by using the result which the approved authority. It is related to ISO/IEC 19790 and ISO/IEC 24759 by providing security requirements for cryptographic modules and test requirements for cryptographic modules.
ISO/IEC 20543	Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408	1st CD	This standard defines evaluation methods and test requirements to perform evaluation and testing of the different types of RBGs defined in ISO/IEC 18031. It complements the existing set of ISO/IEC standards covering cryptographic algorithm and security mechanism testing.
ISO/IEC 20897	Security requirements and test methods for physically unclonable functions for generating non-stored security parameters	3rd WD	This International Standard specifies the security requirements and the test methods for physically unclonable functions for generating non-stored cryptographic parameters.
ISO/IEC 21827	Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)	2nd ed	ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.
ISO/IEC 24759	Test requirements for cryptographic modules	3rd ed	ISO/IEC 24759:2017 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012.

WG 3 Products

Standard	Title	Status	Abstract
ISO/IEC 29128	Verification of cryptographic protocols	1st ed	ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols.
ISO/IEC 29147	Vulnerability Disclosure	1st CD Under revision	ISO/IEC 29147:2014 gives guidelines for the disclosure of potential vulnerabilities in products and online services.
ISO/IEC TS 30104	Physical security attacks, mitigation techniques and security requirements	1st ed	ISO/IEC TS 30104:2015 addresses how security assurance can be stated for products where the risk of the security environment requires the support of physical protection mechanisms.
ISO/IEC 30111	Vulnerability handling processes	1st CD Under revision	ISO/IEC 30111:2013 gives guidelines for how to process and resolve potential vulnerability information in a product or online service. It is applicable to vendors involved in handling vulnerabilities.

WG3 Future Considerations

Topics	Status
Security requirements, test and evaluation methods for White Box Cryptography	Study period

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27035	Information security incident management	1st ed. 2011 (Under revision)	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	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	Information security incident management – Part 2: Guidelines to plan and prepare for incident response	1st Ed. 2016	Describes how to plan and prepare for incident response. This part covers the “Plan and Prepare” and “Lessons Learnt” phases of the model presented in Part 1.
ISO/IEC TS 27035-3	Information security incident management – Part 3: Guidelines for incident response operations	NWIP	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 27036-1	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 security for supplier relationships – Part 2: Requirements	1st ed. 2014 Under process of revision 2017	Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.
ISO/IEC 27036-3	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 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 27037	Guidelines for the identification, collection, acquisition and preservation of digital evidence	1st ed. 2012	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 27041	Guidance on assuring suitability and adequacy of incident investigative methods	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	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	Incident investigation principles and processes	1st ed. 2015	Provides guidelines that encapsulate idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence.
ISO/IEC TR 29149	Best practice on the provision and use of time-stamping services	1st ed. 2012	This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness and data integrity services, or non-repudiation services (in conjunction with other mechanisms). It covers time-stamp services, explaining how to generate, renew, and verify time-stamp tokens.

WG4 Products

Standard	Title	Status	Abstract
ISO/IEC 27050-1	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	Electronic discovery – Part 2: Guidance for governance and management of electronic discovery	3 CD	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	Electronic discovery – Part 3: Code of Practice for electronic discovery	FDIS	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	Electronic discovery – Part 4: ICT readiness for electronic discovery	NWIP	Provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes.

WG4 Future Considerations

Topics	Status
Guidelines for security and privacy in Internet of Things (IoT)	Study period
Big Data security capability maturity model	Study period
Investigation of collaboration with ISO TC 68/SC 2 and development of a NWIP for information security guidance for PKI service providers	Study period
Investigation of need for guidelines on Security Operation Center (SOC)	Study period
Cybersecurity (Joint with WG 1)	Study period
Architecture of Trusted Connection to Cloud Services	Study period

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 (CD)	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	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	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	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 29115	Entity authentication assurance framework	1st ed. 2013 under revision (NP)	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.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors	1st ed. 2014	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.
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.

WG 5 Products

Standard	Title	Status	Abstract
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

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 29003	Identity proofing	PDTS
ITU-T X.gpim | ISO/IEC 29151	Code of practice for personally identifiable information protection	FDIS
ISO/IEC 20889	Privacy enhancing data de-identification techniques	CD
ISO/IEC 29184	Guidelines for online privacy notice and consent	WD
ISO/IEC 27550	Privacy engineering	WD
ISO/IEC 27552	Enhancement to ISO/IEC 27001 for privacy management – Requirements	WD
ISO/IEC 27551	Requirements for attribute-based unlinkable entity authentication	WD
Study Period	PII protection considerations for smartphone App providers	Continuing
Study Period	Privacy in smart cities	Continuing
Study Period	Identity related standards landscape	Continuing
Study Period	Identity assurance framework	Starting
Study Period	Framework of enhanced authentication in telebiometric environments using presentation attack detection mechanisms	Starting
Study Period	Application of ISO 31000 for identity-related risk	Starting
Study Period	Framework of user-centric PII handling based on privacy preference management by users	Starting

Contact Point

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

krystyna.passia@din.de