SC27 STANDING DOCUMENT SD11: 2022 (2)

Overview of SC 27

Structure, Members and Work Programme

July 2022

WELCOME TO SD11: 2022 (2)

ISO/IEC JTC 1/SC 27 is an internationally recognized centre for the development of standards for information security, cybersecurity and privacy protection. The mission of SC 27 is to serve the global needs of all organizations (small, medium and large), as well as governments, non-governmental organizations, academia and society as a whole. Its work covers both management standards as well as technical standards.

The information contained in this publication, SD11, reflects some of the many achievements and developments of SC 27 since its establishment in April 1990. These achievements are a direct result of responding to market and business needs, greater interest in management system security, changes in risks, changes in technology, ubiquitous deployment of wireless and mobile computing and communications, societal security, economic changes and the impact of new regulations. In 2020 marked the 30th birthday of SC 27- a significant stage in the history of information security and privacy standards – a time to reflect on a truly successful chronicle of achievements including the best-selling information security standard ISO/IEC 27001 (ranked 3rd by ISO after ISO 9001 and ISO 14001), the high profile code of practice ISO/IEC 27002 (revised in 2022), the security evaluation criteria ISO/IEC 15408 and the recently published ISO/IEC 27701 (the extension of ISO/IEC 27001 for privacy), as well as many notable crypto standards and prominent service and control standards.

SC 27 continues to engage in standardisation work at the forefront of the marketplace, embracing the requirements of new and emerging technologies and business innovations. The latest developments include work on the security and privacy requirements of the IoT (Internet of Things), Big Data security, trustworthiness and applications involving privacy technology.

SC 27 together with its National Standards Body members, its liaison partners and its experts ensures that its standardisation products provide the best solutions for industry and business.

NOTE: The status of each of the projects listed in the working group tables given in this edition of SD 11 is correct up to 19th May 2022. Updates to these tables will appear in the next edition of SD 11 which is due in 2023.

Dr Edward Humphreys (Convenor SC 27 Communications and Outreach Group AG 07)
Pierre Sasseville (SD 11 editor)
July 2022

CONTENTS

SC 27 SCOPE, STRUCTURE AND MEMBERS

SCOPE OF WORK

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

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

STRUCTURE

JTC 1/SC 27 Chairman: DIN, Germany, Dr. Andreas WOLF

JTC 1/SC 27 Chair-support: ANSI, United States, Laura LINDSAY

JTC 1/SC 27 Communications Officer: BSI, United Kingdom, Dr. Edward HUMPHREYS

JTC 1/SC 27 Committee Manager: DIN, Germany, Sobhi MAHMOUD

JTC 1/SC 27 Secretariat: DIN, Germany

SC 27 WORKING GROUPS

WG 1: Information Security Management Systems

- Convenor: Dr. Edward HUMPHREYS, BSI, United Kingdom
- Convener support: Pablo CORONA, DGN, Mexico
- Convenor support team: Zhigao FU, SAC, China

WG 2: Cryptography and Security Mechanisms

- Convenor: Hirotaka YOSHIDA, JISC, JapanConvenor support: Takeshi CHIKAZAWA, JISC, Japan

WG 3: Security Evaluation, Testing and Specification

- Convenor: Miguel BAÑÓN, UNE, Spain
- Convenor support: Naruki KAI, JISC, Japan

WG 4: Security Controls and Services

- Convenor: Johann AMSENGA, ILNAS, Luxembourg
- Convenor support: François LOREK, AFNOR, France

WG 5: Identity Management and Privacy Technologies

- Convenor: Prof. Dr. Kai RANNENBERG, DIN, Germany
- Convenor support: Dr. Jan SCHALLABÖCK, DIN, Germany

SC 27 ADVISORY GROUPS

AG-1 (Management Advisory Group)

- Convenor: Jean-Pierre QUEMARD, AFNOR, France

AG-2 (Trustworthiness)

- Convenor: Johann AMSENGA, ILNAS, Luxembourg
- Convenor support; Faud KHAN, SCC, Canada

AG-3 (Concepts and Terminology)

- Convenor: Elzbieta ANDRUKIEWICZ, PKN, Poland
- Convenor support: Joanne KNIGHT, NZSO, New Zealand

AG-5 (Strategy)

- Convenor: Jean-Pierre QUEMARD, AFNOR, France

AG-6 (Operations)

- Convenor: Dr. Qin QIU, SAC, China

AG-7 (Communications and Outreach)

- Convenor: Dr. Edward HUMPHREYS, BSI, United Kingdom
- Convenor support: Taewan PARK, KATS, Republic of Korea

SC 27 JOINT WORKING GROUPS

ISO/IEC JTC 1/SC 27/JWG 6 Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices

Convenor: Di TANG, SAC, China (appointed by JTC 1/SC 27)

- Co-Convenor: Gido SCHARFENBERGER-FABIAN, DIN, Germany (appointed by JTC 1/TC22/SC32)

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

- Co-Convenor: Julien BRINGER, AFNOR, France (appointed by ISO/TC 307)
- Co-Convenor: Sal FRANCOMACARO ANSI, USA (appointed by 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 information and IT security standards

Member bodies consists mostly of National Bodies representing countries. Membership types:

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

P-MEMBERS

P-Members are ISO/IEC member bodies that 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:

Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Costa Rica, Côte d' Ivoire, Cyprus, Denmark, Estonia, Finland, France, Germany, India, Indonesia, Islamic Rep. of Iran, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, Rep. of Korea, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Panama, Peru, Philippines, Poland, Russian Federation, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay (Total: 49)

O-MEMBERS

O-members are ISO/IEC member bodies that 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:

Algeria, Belarus, Plurinational State of Bolivia, Bosnia and Herzegovina, Bulgaria, Chile, Croatia, Czech Republic, El Salvador, Eswatini, Ghana, Hong Kong Special Administrative Region of China, Hungary, Iceland, Lebanon, Lithuania, Mauritius, Morocco, North Macedonia, Pakistan, State of Palestine, Portugal, Romania, Rwanda, Saint Kitts and Nevis, Senegal, Serbia, Sri Lanka, State of Palestine, Thailand, Trinidad and Tobago, Turkey, Vietnam (Total: 32)

SC27 LIAISONS

SC27 has liaisons with many other organizations and standards groups both within ISO and IEC and external to ISO and IEC – see https://www.din.de/resource/blob/321664/2b76007acd42ff17a8ecb35c13d77dd1/sc27-liaisons-data.pdf.

MEETING LOCATION HISTORY

ISO/IEC JTC 1/ SC27 has been successfully in operation for 31 years and has been holding its regular 6-monthly meetings in different parts of the world. The full location history of the meetings is summarized as follows.

Year	Meeting Location	Meeting Location
2022		Virtual Meetings via Zoom (April)
2021	Virtual Meetings via Zoom (October)	Virtual Meetings via Zoom (April)
2020	Virtual Meetings via Zoom (September)	Virtual Meetings via Zoom (April)
2019	Paris, France (October)	Tel Aviv, Israel (April)
2018	Gjovik, Norway (September/October)	Wuhan, China (April)
2017	Berlin, Germany (October)	Hamilton, New Zealand (April)
2016	Abu Dhabi, UAE (October)	Tampa, FL, USA (April)
2015	Jaipur, India (October)	Kuching, Sarawak, Malaysia (May)
2014	Mexico City, Mexico (October)	Hong Kong, SAR China (April)
2013	Incheon, Republic of South Korea (October)	Sophia Antipolis, France (April)
2012	Rome, Italy (October)	Stockholm, Sweden (May)
2011	Nairobi, Kenya (November)	Singapore (April)
2010	Berlin, Germany (October)	Melaka, Malaysia (April)
2009	Redmond, Washington, USA (November)	Beijing, China (May)
2008	Limassol, Cyprus (October)	Kyoto, Japan (April)
2007	Lucerne, Switzerland (October)	Moscow/St Petersburg, Russia (May)
2006	Glenburn Lodge, South Africa (November)	Madrid, Spain (May)
2005	Kuala Lumpur, Malaysia (November)	Vienna, Austria (April)
2004	Fortaleza, Brazil (October)	Singapore (April)
2003	Paris, France (October)	Quebec, Canada (April)
2002	Warsaw, Poland (October)	Berlin, Germany (April)
2001	Seoul, Republic of South Korea (October)	Oslo, Norway (April)
2000	Tokyo, Japan (October)	London, UK (April)
1999	Columbia, Maryland, USA (October)	Madrid, Spain (April)
1998	Itacurussa, Brazil (October)	Kista, Sweden (April)
1997	Bad Boll, Germany (October)	Sydney, Australia (April)
1996	Ermatingen, Switzerland (October)	London, UK (April)
1995	Seoul, Republic of South Korea (November)	Helsinki, Finland (April)
1994	Ottawa, Canada (November)	Trondheim, Norway (March)

1993	Paris, France (October)	Milan, Italy (March)
1992	Gaithersburg, Maryland, USA (October)	Zurich, Switzerland (March)
1991	Brussels, Belgium (October)	Tokyo, Japan (April)
1990	Munich, Germany (October)	Stockholm, Sweden (April)

REFERENCES

ISO/IEC SC 27

- https://www.iso.org/committee/45306.html
- https://www.din.de/en/meta/jtc1sc27

JTC 1

- https://www.iso.org/committee/45020.html
- http://www.jtc1.org
- https://jtc1info.org/sd-2-history/jtc1-subcommittees/sc-27/ [History of SC 27]
- https://jtc1info.org/technology/subcommittees/information-security-cybersecurity-privacy-protection/ [SC 27 committee information]

ISO ARTICLES

- Keeping consumers and citizens safe and secure (2021-05-06) https://www.iso.org/news/ref2664.html
- The cybersecurity skills gap (2021-04-15) https://www.iso.org/news/ref2655.html
- Protecting our privacy in smart cities (2021-02-18) https://www.iso.org/news/ref2631.html
- Keeping cybersafe (2021-02-16) https://www.iso.org/news/ref2629.html
- Biometric security (2021-01-14) https://www.iso.org/contents/news/2021/01/Ref2613.html
- Keeping an eye on information security (2020-12-16) https://www.iso.org/news/ref2495.html
- Getting big on data (2020-11-05) https://www.iso.org/news/ref2578.html
- Keeping cyberspace safe for 30 years (2020-10-02) https://www.iso.org/news/ref2563.html
- Safe, secure and private, whatever your business (2020-05-04) https://www.iso.org/news/ref2495.html
- How Microsoft makes your data its priority (2020-03-10) https://www.iso.org/news/ref2489.html
- Guidance for information security management systems auditors just updated (2020-01-27) https://www.iso.org/news/ref2477.html
- Its all about trust (2019-11-11) https://www.iso.org/news/ref2452.html
- Are we safe in the internet of things? (2019-09-05) https://www.iso.org/news/2016/09/Ref2113.html
- Tackling privacy information management head on: first international standard just published (2019-08-06) https://www.iso.org/news/ref2419.html
- Stronger data protection with updated guidelines on assessing information security controls (2019-02-04) https://www.iso.org/news/ref2367.html
- Cracking down on cyber challenges in the latest ISO Focus (2019-01-10) https://www.iso.org/news/ref2363.html
- How to tackle todays IT security risks (2019-01-10) https://www.iso.org/news/ref2360.html
- How to measure the effectiveness of information security (2016-12-16) https://www.iso.org/news/2016/12/Ref2151.html
- Common terminology for information security management just revised (2016-02-18)

https://www.iso.org/news/2016/02/Ref2048.html

- Security toolbox protects organizations from cyber-attacks (2015-12-17) https://www.iso.org/news/2015/12/Ref2032.html
- IT security experts win technical excellence award (2015-09-17) https://www.iso.org/news/2015/09/Ref2005.html
- Safeguard your information with new IT security collection (2013-11-18) https://www.iso.org/news/2013/11/Ref1799.html
- Are you prepared for information security breaches? new ISO/IEC 27001 can help (2013-10-04) https://www.iso.org/news/2013/10/Ref1783.html
- New version of ISO/IEC 27001 to better tackle IT security risks (2013-08-14) https://www.iso.org/news/2013/08/Ref1767.html

IEC ARTICLES

- Cyber security for IT and OT supply chains (2021-02-03) https://www.iec.ch/blog/cyber-security-it-and-ot-supply-chains
- Securing IT and OT supply chains with international standards and conformity assessment (2021-02-01) https://etech.iec.ch/issue/2021-01/securing-it-and-ot-supply-chains-with-international-standards-and-conformity-assessment
- https://etech.iec.ch/issue/2020-03/effective-governance-is-the-key-to-cyber-security
- https://etech.iec.ch/issue/2020-02/eight-things-organizations-should-do-to-ensure-compliance-with-cyber-security-regulations

ABBREVIATIONS

JTC 1	joint technical committee one
SC	sub-committee
WG	working group
AG	advisory group
PWI	preliminary work item
WD	working draft
CD	committee draft
DIS	draft international standard
FDIS	final draft international standard
IS	international standard
TS	technical specification
TR	technical report
SD	standing document

SC 27 WORKING GROUPS

WG 1 INFORMATION SECURITY MANAGEMENT SYSTEMS

- Convenor: Dr. Edward HUMPHREYS, BSI (GB)
- Convener Support: Pablo CORONA FRAGA, DGN (MX)
- Convenor Support Team: Zhigao FU, SAC (CN)

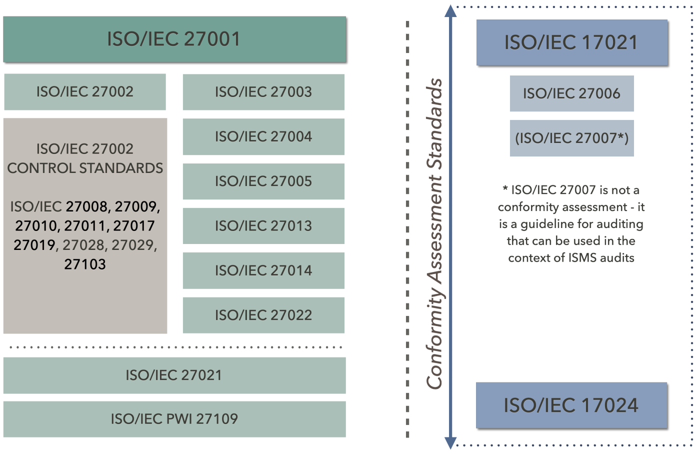
SCOPE

WG 1 is the centre of international expertise on standardization matters regarding all aspects of information security management system (ISMS) standards and management system issues related to the protection of information. The scope of WG 1 covers the development of ISMS standards and guidelines, including the following:

- Development and maintenance of the ISO/IEC 27000 ISMS standards family (see figure);
- Identification of requirements for future ISMS standards and guidelines;
- Collaboration with other Working Groups in SC 27, in particular with WG 4 and WG 5 on standards addressing the implementation of ISMS requirements and controls ~~and controls~~ as defined in ISO/IEC 27001 and ISO/IEC 27002;
- On-going maintenance of WG 1 standing documents, including SD1 (WG 1 Roadmap), and
  SD2 (Guidance on terminology processes);
- Liaison and collaboration with those organizations and committees with an interest in ISMS standards and guidelines.

The following aspects may be distinguished as within scope and responsibility of WG 1:

- Information security management system (ISMS) requirements;
- ISMS guidelines and supporting implementation documentation, for example, for ISMS information security management measurements, information security risk management;
- ISMS accreditation, certification requirements and auditing standards;
- Sector and application specific ISMS control standards;
- Competence requirements standards for ISMS professionals;
- Information security management governance;
- Cybersecurity;
- Cross-sector/application integration of management system standards e.g. ISO/IEC 27013;
- Information security and ISMS definitions and terminology.


ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27002 CONTROL STANDARDS
ISO/IEC 27008, 27009, 27010, 27011, 27017 27019, 27028, 27029, 27103
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC 27022
ISO/IEC 27021
ISO/IEC PWI 27109
Conformity Assessment Standards
ISO/IEC 17021
ISO/IEC 27006
(ISO/IEC 27007*)
* ISO/IEC 27007 is not a conformity assessment - it is a guideline for auditing that can be used in the context of ISMS audits
ISO/IEC 17024

WG 1 also has a Conformity Assessment Task Force (CATF) that develops advisory notes on all aspects of conformity assessment that apply to SC 27 standards. Furthermore, WG 1 has liaisons with IAF and TMB JTCG, and with CASCO/CAB (through the SC 27 liaison officer).

Standard	Title	Status	Abstract
ISO/IEC 27000	Overview and vocabulary	2018 (edition 5) Under revision PWI	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	2013 (edition 2) Cor 1: 2014 Cor 2: 2015 Under revision (FDIS) - edition 3 planned for Q3 2022	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 business activities of the organization and the risks it faces.
ISO/IEC 27002	Information security controls	2022 (edition 3)	This International Standard provides a reference set of generic information security controls including implementation guidance.
ISO/IEC 27003	Information security management system - Guidance	2017 (edition 2)	This document provides explanation and guidance on ISO/IEC 27001:2013
ISO/IEC 27004	Information security management - Monitoring, measurement, analysis and evaluation	2016 (edition 2)	This document provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: a) the monitoring and measurement of information security performance; b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; c) the analysis and evaluation of the results of monitoring and measurement.
ISO/IEC 27005	Information security risk management	2018 (edition 3) Under revision (FDIS)	This International Standard provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is

Standard	Title	Status	Abstract
			designed to assist the satisfactory implementation of information security based on a risk management approach.
ISO/IEC 27006-1	Requirements for bodies providing audit and certification of information security management systems — Part 1: General	2016 (edition 3) AMD1: 2020 Under revision (DIS)	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	2020 (edition 3)	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 the assessment of information security controls	2019 (edition 1) Under revision PWI	This Technical Report provides guidance for assessing the implementation of ISMS controls determined 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.
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements	2020 (edition 2) Under revision PWI	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.

Standard	Title	Status	Abstract
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications	2015 (edition 2)	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-organizational and inter-sector communications.
ITU-T X.1051 | ISO/IEC 27011	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	2016 (edition 2) Cor 1:2018 Under revision (DIS)	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.
ISO/IEC 27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	2021 (edition 3)	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	2022 (edition 2)	This International Standard provides guidance on the development and use of governance of information security (GIS) through which organizations 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 organizations on the effective, efficient, and acceptable use of information security within their organizations.

Standard	Title	Status	Abstract
ISO/IEC TR 27016	Information security management – organisationalOrganisational economics	2014 (edition 1)	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	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	2015 (edition 1) Under revision PWI	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.
ISO/IEC 27019	Information security controls for the energy utility industry	2017 (edition 1) Under revision PWI	This document provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.
ISO/IEC 27021	Competence requirements for information security management systems professionals	2017 (edition 1) AMD1	This document specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving one or more information security management system processes that conforms to ISO/IEC 27001.
ISO/IEC TS 27022	Guidance on information security management system processes	2021 (edition 1)	An information security management system (ISMS) consists of interacting processes and is operated by performing those processes. This document provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them.

Standard	Title	Status	Abstract
ISO/IEC TR 27023	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	2015 (edition 1)	This document provides a mapping between the 2013 editions of ISO/IEC 27001 and ISO/IEC 27002 and the 2005 editions of these standards.
ISO/IEC TR 27024	Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements	TRAWI	
PWI 27028	Guidance on ISO/IEC 27002 attributes	PWI	
PWI 27029	ISO/IEC 27002 and ISO and IEC standards	PWI	
ISO/IEC TS 27100	Cybersecurity – Overview and concepts	2021 TS(edition 1)	This document provides an overview of cybersecurity. This document: — describes cybersecurity and relevant concepts, including how it is related to and different from information security; — establishes the context of cybersecurity; — does not cover all terms and definitions applicable to cybersecurity; and — does not limit other standards in defining new cybersecurity-related terms for use.

Standard	Title	Status	Abstract
ISO/IEC 27102	Guidelines for cyber-insurance	2019 (edition 1)	This document provides guidelines when considering purchasing cyber-insurance as a risk treatment option to manage the impact of a cyber-incident within the organization's information security risk management framework. This document gives guidelines for: • a) considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks; • b) leveraging cyber-insurance to assist manage the impact of a cyber-incident; • c) sharing of data and information between the insured and an insurer to support underwriting, monitoring and claims activities associated with a cyber-insurance policy; • d) leveraging an information security management system when sharing relevant data and information with an insurer. • This document is applicable to organizations of all types, sizes and nature to assist in the planning and purchase of cyber-insurance by the organization.
ISO/IEC TR 27103	Cyber security and ISO and IEC standards	2018 (edition 1) Under revision PWI	This document provides guidance on how to leverage existing standards in a cybersecurity framework.
ISO/IEC TR 27109	Cyber education and training	TRAWI	This preliminary work item is considering the development of a technical report on cyber education.
ISO/IEC TS 27110	Cybersecurity framework development guidelines	2021 (edition 1)	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.

SD	Title
SD 2	Guidance on terminology processes

WG 2 CRYPTOGRAPHY AND SECURITY MECHANISMS

- Convenor: Hirotaka YOSHIDA, JISC (JP)
- Convener Support: Takeshi CHIKAZAWA, JISC (JP)

SCOPE

WG 2 provides a centre of expertise for the standardisation of IT Security techniques and mechanisms within JTC 1 with the following scope:

- Identification of the needs and requirements for these techniques and mechanisms in IT systems and applications;
- Development of terminology, general models and standards for these techniques and mechanisms for use in security services;
- On-going maintenance of WG 2 standing document SD1 (WG 2 Roadmap).

The scope covers both cryptographic and non-cryptographic techniques and mechanisms including:

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

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

Standard	Title	Status	Abstract
ISO/IEC 4922-1	Secure multiparty computation Part 1: General	Under development	ISO/IEC 4922 specifies cryptographic mechanisms to compute a function on data while the data is kept secret, and their properties.
ISO/IEC 4922-2	Part 2: Mechanisms based on secret sharing	Under development	
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 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.
ISO/IEC 9796-3	Part 3: Discrete logarithm based mechanisms	2nd ed. 2006	
ISO/IEC 9797-1	Message authentication codes (MACs) Part 1: Mechanisms using a block cipher	2nd ed. 2011 (+Amd 1)	ISO/IEC 9797 specifies message authentication code (MAC) algorithms, which are data integrity mechanisms that compute a short string
ISO/IEC 9797-2	Part 2: Mechanisms using a dedicated hash-function	3rd ed. 2021	
ISO/IEC 9797-3	Part 3: Mechanisms using a universal hash-function	1st ed. 2011	
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.
ISO/IEC 9798-2	Part 2: Mechanisms using symmetric encipherment algorithms	4th ed. 2019	

Standard	Title	Status	Abstract
ISO/IEC 9798-3	Part 3: Mechanisms using digital signature techniques	3rd ed. 2019	
ISO/IEC 9798-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
ISO/IEC 9798-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009	
ISO/IEC 9798-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	
ISO/IEC 10116	Modes of operation for an n-bit block cipher algorithm	4th ed. 2017 (+Amd 1)	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 (+Amd 1)	ISO/IEC 10118 specifies some kinds of hash-functions which map arbitrary strings of bits to a given range.
ISO/IEC 10118-2	Part 2: Hash-functions using an n-bit block cipher	3rd ed. 2010	
ISO/IEC 10118-3	Part 3: Dedicated hash-functions	4th ed. 2018	
ISO/IEC 10118-4	Part 4: Hash-functions using modular arithmetic	1st ed. 1998 (+Amd 1)	
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
ISO/IEC 11770-2	Part 2: Mechanisms using symmetric techniques	3rd ed. 2018	
ISO/IEC 11770-3	Part 3: Mechanisms using asymmetric techniques	4th ed. 2021	

Standard	Title	Status	Abstract
ISO/IEC 11770-4	Part 4: Mechanisms based on weak secrets	2nd ed. 2017 (+Amd 1/2)	
ISO/IEC 11770-5	Part 5: Group key management	2nd ed. 2020	
ISO/IEC 11770-6	Part 6: Key derivation	1st ed. 2016	
ISO/IEC 11770-7	Part 7: Cross-domain password-based authenticated key exchange	1st ed. 2021	
ISO/IEC 13888-1	Non-repudiation Part 1: General	4th ed. 2020	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.
ISO/IEC 13888-2	Part 2: Mechanisms using symmetric techniques	2nd ed. 2010	
ISO/IEC 13888-3	Part 3: Mechanisms using asymmetric techniques	3rd ed. 2020	
ISO/IEC 14888-1	Digital signatures with appendix Part 1: General	2nd ed. 2008	ISO/IEC 14888 specifies digital signature mechanisms with appendix.
ISO/IEC 14888-2	Part 2: Integer factorization based mechanisms	2nd ed. 2008	
ISO/IEC 14888-3	Part 3: Discrete logarithm based mechanisms	3rd ed. 2016	
ISO/IEC 14888-4	Part 4: Stateful hash-based mechanisms	Under development	
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

Standard	Title	Status	Abstract
ISO/IEC 15946-5	Part 5: Elliptic curve generation	2nd ed. 2017 Under revision	techniques.
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.
ISO/IEC 18014-2	Part 2: Mechanisms producing independent tokens	3rd ed. 2021	
ISO/IEC 18014-3	Part 3: Mechanisms producing linked tokens	2nd ed. 2009	
ISO/IEC 18014-4	Part 4: Traceability of time sources	1st ed. 2015	
ISO/IEC 18031	Random bit generation	2nd ed. 2011 (+Amd1) Under revision	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	2nd ed. 2020	ISO/IEC 18032 presents methods for generating prime numbers as required in cryptographic protocols and algorithms.
ISO/IEC 18033-1	Encryption algorithms Part 1: General	2nd ed. 2021	ISO/IEC 18033 specifies asymmetric ciphers (including identity-based ciphers, homomorphic encryption, fully homomorphic encryption) and symmetric ciphers (block ciphers and stream ciphers).
ISO/IEC 18033-2	Part 2: Asymmetric ciphers	1st ed. 2006 (+Amd 1)	
ISO/IEC 18033-3	Part 3: Block ciphers	2nd ed. 2010 (+Amd 1)	
ISO/IEC 18033-4	Part 4: Stream ciphers	2nd ed. 2011 (+Amd 1)	
ISO/IEC 18033-5	Part 5: Identity-based ciphers	1st ed. 2015 (+Amd 1)	
ISO/IEC 18033-6	Part 6: Homomorphic encryption	1st ed. 2019	
ISO/IEC 18033-7	Part 7: Tweakable block ciphers	1st ed. 2022	

Standard	Title	Status	Abstract
ISO/IEC 18033-8	Part 8: Fully homomorphic encryption	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.
ISO/IEC 18370-2	Part 2: Discrete logarithm based mechanisms	1st ed. 2016	
ISO/IEC 19592-1	Secret sharing Part 1: General	1st ed. 2016	ISO/IEC 19592 describes cryptographic secret sharing schemes and their properties.
ISO/IEC 19592-2	Part 2: Fundamental mechanisms	1st ed. 2017	
ISO/IEC 19772	Authenticated encryption	2nd ed. 2020	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 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.
ISO/IEC 20008-2	Part 2: Mechanisms using a group public key	1st ed. 2013 (+Amd 2)	
ISO/IEC 20008-3	Part 3: Mechanisms using a group public key	Under development	
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.
ISO/IEC 20009-2	Part 2: Mechanisms based on signatures using a group public key	1st ed. 2013	
ISO/IEC 20009-3	Part 3: Mechanisms based on blind signatures	Under development	

Standard	Title	Status	Abstract
ISO/IEC 20009-4	Part 4: Mechanisms based on weak secrets	1st ed. 2017	
ISO/IEC 23264-1	Redaction of authentic data Part 1: General	1st ed. 2021	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.
ISO/IEC 23264-2	Part 2: Redactable signature schemes based on asymmetric mechanisms	Under development	
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 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.
ISO/IEC 29192-2	Part 2: Block ciphers	2nd ed. 2019	
ISO/IEC 29192-3	Part 3: Stream ciphers	1st ed. 2012	
ISO/IEC 29192-4	Part 4: Mechanisms using asymmetric techniques	1st ed. 2013	
ISO/IEC 29192-5	Part 5: Hash-functions	1st ed. 2016	
ISO/IEC 29192-6	Part 6: Message authentication codes (MACs)	1st ed. 2019	
ISO/IEC 29192-7	Part 7: Broadcast authentication protocols	1st ed. 2019	

Standard	Title	Status	Abstract
ISO/IEC 29192-8	Part 8: Authenticated encryption	Under development	
PWI 29004	Modes of operation for tweakable block ciphers	PWI	
PWI 13025	Inclusion of arithmetization-friendly cryptographic algorithms in ISO/IEC standards	PWI	
PWI 13035	Amendment of Identity-Based Authenticated Key Exchange	PWI	
PWI 13042	Consideration of the Security Model for Mechanism 7a in ISO/IEC 9798-6	PWI	

WG 3 SECURITY EVALUATION, TESTING AND SPECIFICATION

- Convener: Miguel BAÑÓN, UNE (ES)
- Convenor-support: Naruki KAI, JISC (JP)

SCOPE

The scope of WG 3 covers aspects related to security engineering with particular emphasis on, but not limited to, standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. This includes consideration of computer networks, distributed systems, associated application services, biometrics.

The following aspects may be distinguished:

- security evaluation criteria;
- methodology for application of the criteria;
- security functional and assurance specification of IT systems, components and products;
- testing methodology for determination of security functional and assurance conformance;
- administrative procedures for testing, evaluation, certification, and accreditation schemes;
- On-going maintenance of WG 3 standing document SD1 (WG 3 Roadmap).

The work reflects the needs of relevant sectors in society, as represented through ISO/IEC National Bodies and other organizations in liaison, expressed in standards for security functionality and assurance.

Account is taken of related ISO/IEC and ISO standards for quality management and testing so as not to duplicate these efforts.

Standard	Title	Status	Abstract
ISO/IEC TR 5891	A General Framework for Runtime Hardware Security Assessment	Under development Submitted for publication	This TR describes a possible security assessment methodology whereby the runtime behaviours of one or more hardware components in post-silicon phase could be verified by an agent that is external to the hardware components.
ISO/IEC TR 5895	Multi-party coordinated vulnerability disclosure and handling	Under development Submitted for publication	This TR clarifies and augments the application and implementation of ISO/IEC 30111 and ISO/IEC 29147 in multi-party coordinated vulnerability disclosure (MPCVD) settings, including the evolving commonly adopted practices in this area.
ISO/IEC TS 9569	Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045	Under development WD stage	This Technical Specification will collect the discussions and experience from the ISO/IEC 15408 and ISO/IEC 18045 experts interested in the solution of the Patch Management problem. The document will propose a way to solve the problem in a harmonized but not yet standardized way.
ISO/IEC 15408	Evaluation criteria for IT security	Under revision Submitted for publication	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: P Introduction and general model Q Security functional components R Security assurance components S Framework for the specification of evaluation methods and activities T Pre-defined packages of security requirements
ISO/IEC TR 15443	Security Assurance Framework	2nd 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.

Standard	Title	Status	Abstract
ISO/IEC TR 15446	Guide for the preparation of Security Targets and Protection Profiles	3rd Ed 2017	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	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	Under revision CD stage	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	Under revision Submitted for publication	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.
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 (PII). This document analyses those principles and maps them, where possible, to the security functional requirements defined in ISO/IEC 15408-2.
ISO/IEC 19790	Security requirements for cryptographic modules	Under revision WD stage	ISO/IEC 19790 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems

Standard	Title	Status	Abstract
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	Under revision WD stage	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	Under revision WD stage	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	1st Ed 2020	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.
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.

Standard	Title	Status	Abstract
ISO/IEC 20085	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules	1st Ed 2019 part 1, 2020 part 2.	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	Guidelines for testing cryptographic modules in their operational environment	1st Ed 2018 PWI initiated	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	Physically unclonable functions	ISO/IEC 20897-1 1st Ed 2020 ISO/IEC 20897-2 Submitted for publication	This project will specify 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. 2008	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 21827:2008 does not prescribe a particular process or sequence, but captures practices generally observed in industry.
ISO/IEC TR 22216	Introductory guidance on evaluation for IT security	1st Ed. 2022	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.

Standard	Title	Status	Abstract
ISO/IEC TS 23532	Requirements for the competence of IT security testing and evaluation laboratories	1st Ed. 2021	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 DIS stage	ISO/IEC 23837 specifies the security requirements, test and evaluation methods for Quantum Key Distribution (QKD) under the framework of ISO/IEC 15408. QKD provides a method to use a pre-shared key for establishing a symmetric key with information theoretic security. The established key can be subsequently used with an information theoretic secure encryption mechanism to create a secure communication channel. To achieve such a high level of security the implementation of the system and the security primitives should satisfy criteria that are given in this document.
ISO/IEC TS 24462	Ontology for ICT Trustworthiness Assessment	Under revision WD stage	The proposed Technical Specification will define an inventory of building blocks conceptually associated with different types of assessments, an ontology (i.e., a meta-model) that organizes the building blocks, and guidelines for using the inventory of building blocks and the ontology. The ontology will cover the domain of ICT assessment and define a consistent view in this space.
ISO/IEC TR 24485	Security properties, test and evaluation guidance for white box cryptography	Under development DTR stage	This Technical Report introduces security properties and provides guidance on the test and the evaluation of white box cryptography (WBC), that is a cryptographic algorithm specialized for a key, but where the said key cannot be extracted.
ISO/IEC 24759	Test requirements for cryptographic modules	Under revision WD stage	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	Under revision	ISO/IEC 29128 provides a technical base for the assessment of the security of cryptographic protocols.

Standard	Title	Status	Abstract
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	ISO/IEC 30111 gives guidelines for how to process and resolve potential vulnerability information reported by individuals or organizations that find a potential vulnerability.

WG 4 SECURITY CONTROLS AND SERVICES

- Convener: Johann AMSENGA, ILNAS (LU)
- Convener-support: François LOREK, AFNOR (FR)

SCOPE

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.

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	2nd 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 confirmed in 2018	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 confirmed in 2020	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.

Standard	Title	Status	Abstract
ISO/IEC 27035-1 (Under 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 27035-1	Information technology – Information security incident management – Part 1: Principles and process	2nd CD	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 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, and lessons learned from 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 27035-2	Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response	2nd CD	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 ICT incident response operations	1st ed. 2020	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,

Standard	Title	Status	Abstract
			and response activities for the collected data or security events.
ISO/IEC 27035-4	Information technology – Information security incident management – Part 4: Coordination	3rd WD	This part of ISO/IEC 27035 provides the guidelines for coordination among IRTs of multiple organizations to work together to handle information security incidents. It also addresses the impacts by working together to the internal incident management of one organization, and provides guidelines for individual IRT to adapt to the coordination process. Furthermore, it provides guidelines for the coordination team, if exists, to perform supporting coordination activities.
ISO/IEC 27041	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method	1st ed. 2015 Confirmed in 2021	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 Confirmed in 2021	Provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility and repeatability.

Standard	Title	Status	Abstract
ISO/IEC 27043	Information technology – Security techniques – Incident investigation principles and processes	1st ed. 2015 confirmed in 2020	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.
ISO/IEC 27050-1	Information technology Electronic discovery – Part 1: Overview and concepts	2nd ed. 2019	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 – Electronic discovery – Part 3: Code of practice for electronic discovery	2nd ed. 2020	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 ed. 2021	Provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes.

Standard	Title	Status	Abstract
ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts	2nd ed. 2015 Confirmed in 2021	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 2018	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 Confirmed in 2019	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 Confirmed in 2019	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 –	1st ed. 2016 Confirmed in	Describes the threats, security requirements, security control

Standard	Title	Status	Abstract
	Network security – Part 6: Securing wireless IP network access	2021	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.
ISO/IEC 27033-7	Information technology – Network security – Part 7: Guidelines for network virtualization security	4th WD	This document aims to identify security risks of network virtualization, and propose guidelines for implementation of network virtualization security.
ISO/IEC 27036-1 (under minor revision)	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/i ndex.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 27036-1	Cybersecurity – Supplier relationships – Part 1: Overview and concepts	FDIS	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 (under revision)	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.

Standard	Title	Status	Abstract
ISO/IEC 27036-2	Cybersecurity – Supplier relationships – Part 2: Requirements	DIS	Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.
ISO/IEC 27036-3 (under early revision)	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 27036-3	Cybersecurity – Supplier relationships – Part 3: Guidelines for information and communication technology supply chain security	2nd CD	Provides product and service acquirers and suppliers in ICT supply chain with guidance.
ISO/IEC 27036-4 (under periodical review)	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.
ISO/IEC 27038	Information technology – Security techniques – Specification for digital redaction	1st Ed. 2014 Confirmed in 2019	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.

Standard	Title	Status	Abstract
ISO/IEC 27040 (Under revision)	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 27040	Information technology – Storage security	3rd WD	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 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 Confirmed in 2021	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	1st PWI	Provides a detailed description of an Application security validation process used to audit and verify Application Security.

Standard	Title	Status	Abstract
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).
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 Confirmed in 2021	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 (under periodical review)	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.
ISO/IEC 27045	Information technology – Big data security and privacy – Processes	2nd PWI	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.

Standard	Title	Status	Abstract
ITU-T X.842 | ISO/IEC TR 14516	Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services	1st ed. 2002 Confirmed in 2013	Identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public.
ITU-T X.841 | ISO/IEC 15816	Information technology – Security techniques – Security information objects for access control	1st ed. 2002 Confirmed in 2013	Provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality.
ITU-T X.843 | ISO/IEC 15945	Information technology – Security techniques – Specification of TTP services to support the application of digital signatures	1st ed. 2002 Confirmed in 2013	Defines the services required to support the application of digital signatures for non-repudiation of creation of a document.
ISO/IEC 27070	Information technology – Security techniques – Requirements for establishing virtualized roots of trust	DIS	Specifies the security requirements for establishing virtualized roots of trust.
ISO/IEC TR 29149	Information technology – Security techniques – Best practices for the provision and use of time-stamping services	1st ed. 2012 Confirmed in 2018	This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness, data integrity services, and non-repudiation services in conjunction with other mechanisms. It covers time-stamp services, explaining how to generate, renew, and verify time-stamp tokens.
ISO/IEC 27099	Information technology – Public key infrastructure – Practices and policy framework	3rd CD	This document sets out a framework of requirements to manage information security for PKI Trust Service Providers through Certificate Policies, Certificate Practice Statements, and, where applicable, their internal underpinning by an ISMS. The framework of

Standard	Title	Status	Abstract
			requirements includes the assessment and treatment of information security risks, tailored to meet the agreed service requirements of its users as specified through the certificate policy.
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII	1st ed. 2019	Specifies the Security and Privacy aspects of Service Level Agreements (SLA) for cloud services including requirements and guidance.
ISO/IEC 20547-4	Information technology – Big Data Reference Architecture – Part 4: Security and Privacy	1st ed. 2020	Specifies the underlying Security and Privacy fabric that applies to all aspects of the BDRA (Big Data Reference Architecture) including the Big Data roles, activities, and functional components.
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for the design and implementation of virtualized servers	1st ed. 2018	Specifies security guidelines for the design and implementation of virtualized servers. It is not applicable to: desktop, network and storage virtualization, or to vendor attestation.
ISO/IEC 27032 (under revision)	Information technology – Security techniques – Guidelines for cybersecurity	1st ed. 2012 Confirmed in 2018	Provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains. It covers the baseline security practices for stakeholders in the Cyberspace.
ISO/IEC 27032	Information technology – Cybersecurity – Guidelines for Internet security	2nd CD	Focus is to address internet security issues and provides technical guidance for addressing common internet security risks.
ISO/IEC 5689	Security reference architecture for cyber-physical systems (CPS)	5th PWI	This document provides a security reference architecture for cyber-physical systems based on identified security concerns.

Standard	Title	Status	Abstract
ISO/IEC 4983	Information technology – Security techniques – Secure deployment, updating, and upgrading	2nd WD	This International Standard provides guidance to end user organisations of systems in respect of remedial updating. Its application should result in: - Increased information security of systems - Increased understanding by end user organisations of the risks associated with failing to update systems to enhance the implementation of information security requirements.
ISO/IEC 5181	Data provenance – Reference model	4th PWI	This preliminary work item defines a data provenance reference model for describing and encapsulating the appropriate granularity and layers of data provenance in and across computing environments. The reference model covers both standalone and distributed computing topologies.
ISO/IEC 5192	Guidelines on Security Operations Centers (SOC)	1st PWI	The aim of this work is to establish the viability of having an international standard to address guidelines on Security Operations Centres (SOC). Should the WG find this to be the case, only then a NWIP could be proposed.
ISO/IEC 24392	Information technology – Security techniques – Security reference model for industrial internet platform	1st CD	This standard specifies the security reference model of the industrial Internet platforms, including the various industrial elements of the industrial Internet platforms and their corresponding security responsibilities. It puts forward universal requirements for the

Standard	Title	Status	Abstract
			security of industrial Internet platforms.
ISO/IEC 27046	Information technology – Big data security and privacy – Guidelines for implementation	3rd WD	This document aims to analyze key challenges and risks of big data security and privacy, and propose guidelines for implementation of big data security and privacy in aspects of big data resources, and organizing, distributing, computing and destroying big data.
ISO/IEC 27071	Information technology – Security techniques – Security recommendations for establishing trusted connections between devices and services	1st CD	This International Standard provides a framework and recommendations for establishing trusted connection between device and service based on hardware security modules, including recommendations for components such as: hardware security module, roots of trust, identity, authentication and key establishment, environment attestation, data integrity and authenticity.
ISO/IEC 27400	Cybersecurity – IoT security and privacy – Guidelines	DIS	Provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT)
ISO/IEC 27402	Cybersecurity – IoT security and privacy – Device baseline requirements	2nd CD	This document provides baseline requirements for IoT devices to support information security and privacy controls. This document covers IoT devices that have a network interface.

Standard	Title	Status	Abstract
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	1st CD	This document provides guidelines to analyze security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.
ISO/IEC TR 6114	Information technology – Security techniques – Security assurance throughout system life cycle	3rd WD	To be determined.
ISO/IEC 6109	Data life cycle log audit guidelines	5th PWI	As the basis of security audit and traceability analysis, log records generated by data processing activities is an important part of data security. However, the current log management, use and audit lack of normative guidance for the whole life cycle of data, and it is difficult to effectively find data security risks, trace and analyze data security incidents. According to different data activities, this standard can study the contents, use methods and protection strategies of log records in each stage of data life cycle, and propose log audit guidelines to improve data security.
ISO/IEC 7699	Guidance for addressing security threats and failures in artificial intelligence	2nd PWI	This PWI proposes to standardize guidance for organizations that use or develop artificial intelligence (AI) systems to address failures of such systems as a result of security threats. AI systems can fail in a number of ways as a result of security attacks which can exploit vulnerabilities in AI systems due to the way they are developed and their heavy reliance on data. It is proposed

Standard	Title	Status	Abstract
			to describe the failures of AI systems and how these are caused by various threats and the exploitation of vulnerabilities. The intention is to identify which measures are necessary to address the security of AI systems by first identifying the threats to AI systems as well as the failures these threats cause to help the users and developers of AI systems understand security issues related to AI.
ISO/IEC 7709	Security and privacy reference architecture for multi-party data fusion and mining	2nd PWI	This proposal aims to provide a security and privacy preserving reference architecture of multi-party data fusion and mining. With combination of different secure function components and mechanisms, it targets to reducing risks for data fusion and mining process, it will give the stake holders a clear and comprehensive view for safeguarding and systematic security enhancement.

WG 5 IDENTITY MANAGEMENT AND PRIVACY TECHNOLOGIES

- Convenor: Prof Dr Kai RANNENBERG, DIN (DE)
- Convenor-support: Dr Jan SCHALLABÖCK, DIN (DE)

SCOPE

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

- Identification of requirements for and development of future standards and guidelines in these areas. For example
    - In the area of Identity Management, topics such as:
        - A framework for Identity management;
        - Anonymity and pseudonymity;
        - Credentials and attributes;
        - Entity assurance and Identity proofing;
        - Access management;
    - In the area of Privacy, topics such as:
        - A privacy framework;
        - A privacy reference architecture;
        - Privacy infrastructures;
        - Privacy impact assessment;
        - Specific Privacy Enhancing Technologies (PETs);
        - Privacy engineering;
    - In the area of Biometrics, topics such as:
        - Protection of biometric data;
        - Authentication techniques.
- On-going maintenance of WG 5 standing documents such as SD1 (WG 5 Roadmap), SD2 (Privacy references list), and SD4 (Standards Privacy Assessment (SPA));
- Collaboration with other WGs in SC 27, e.g., WG 1 on management aspects, WG 2 on specific cryptographic techniques, WG 3 on evaluation aspects, WG 4 on specific technologies, and the Joint ISO/TC 307 - JTC 1/SC 27 JWG 4 "Blockchain and distributed ledger technologies and IT Security techniques" on e.g. DLT systems for identity management and privacy and PII protection considerations;
- Liaison and collaboration with those organizations and committees dealing with specific requirements and guidelines for services and applications in this area.

Standard	Title	Status	Abstract
ISO/IEC 24760-1	A framework for identity management – Part 1: Terminology and concepts	2^{nd} ed. 2019 Freely available via jtc1.org Amendment in development (DAmd1)	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 that 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.

Standard	Title	Status	Abstract
ISO/IEC 24760-2	A framework for identity management – Part 2: Reference architecture and requirements	1st ed. 2015 Under revision (CD)	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 Amendment in development (DAmd1)	ISO/IEC 24760-3 provides practices for identity management, e.g. for assurance in identity information use, and controlling the access to identity information.
ISO/IEC 24760-4	A framework for identity management – Part 4: Authenticators, Credentials and Authentication	NP	ISO/IEC 24760-4 provides guidance on implementing user authentication and the use of credentials therein, in particular it: • describes complementary models for implementing authentication with different operational aspects, • specifies formal descriptions of authentication methods, • specifies requirements for authenticators as credentials, • managing the lifecycle, • binding to a principal, • use in a federated context.

Standard	Title	Status	Abstract
ISO/IEC 29100	Privacy framework	1st ed. 2011 Freely available via jtc1.org	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 29100 Amd 1	Privacy framework – Amendment 1: Clarifications	1st ed. 2018	

Standard	Title	Status	Abstract
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.

Standard	Title	Status	Abstract
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.
ISO/IEC 24745	Biometric information protection	2nd ed. 2022	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.

Standard	Title	Status	Abstract
ISO/IEC 24761	Authentication context for biometrics	2nd ed. 2019	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 TS 27006-2 (previously 27558)	Requirements for bodies providing audit and certification of information security management systems – Part 2: Requirements for bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC 27001	1st ed. 2021 Under revision towards an IS (CD)	ISO/IEC 27006 sets out criteria for bodies operating audit and certification of information security management systems. If such bodies are to be accredited as complying with ISO/IEC 27006 with the objective of auditing and certifying privacy information management systems (PIMS) in accordance with ISO/IEC 27701:2019, some additional requirements and guidance to ISO/IEC 27006 are necessary. These are provided by this document. The text in this document follows the structure of ISO/IEC 27006; the additional ISMS-specific requirements and guidance on the application of ISO/IEC 27006 for ISMS certification are identified by the letters "PS".

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

Standard	Title	Status	Abstract
ISO/IEC TR 27550	Privacy engineering for system life cycle processes	1st ed. 2019	ISO/IEC TR 27550 provides privacy engineering guidelines 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 and security engineering, risk management); • privacy engineering activities in key engineering processes such as knowledge and risk management, requirement analysis, and architecture design. The audience includes all 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 27551	Requirements for attribute-based unlinkable entity authentication	1st ed. 2021	Internet sites often collect more than necessary information during the PII principal' s access to the service thus making it possible to link visits from the same PII principal to different sites or to link two or more visits from the same PII principal to the same site. To overcome this issue ISO/IEC 27551 provides a framework and establishes requirements for attribute-based unlinkable entity authentication.

Standard	Title	Status	Abstract
ISO/IEC 27553-1	Security and Privacy requirements for authentication using biometrics on mobile devices – Part 1: Local modes	DIS	This document provides high-level security and privacy requirements for authentication using biometrics on mobile devices, including security and privacy requirements for functional components and for communication. This document is applicable to the cases that the biometric data and derived biometric data does not leave the device, i.e., local modes.
ISO/IEC 27553-2	Security and Privacy requirements for authentication using biometrics on mobile devices – Part 2: Remote modes	NP	This document provides high-level security and privacy requirements for authentication using biometrics on mobile devices, including security and privacy requirements for functional components, for communication and for remote processing. This document is applicable to remote modes, i.e., the cases that: • the biometric sample is captured through mobile devices; • the biometric data or derived biometric data are transmitted between the mobile devices and the remote services in either or both directions. The cases that the biometric data or derived biometric data never leave the mobile devices (i.e., local modes) are out of scope for this document.

Standard	Title	Status	Abstract
ISO/IEC 27554	Application of ISO 31000 for assessment of identity-related risk	CD	This document defines identity-related risk for the purposes of applying ISO 31000 risk management guidelines to this field. It also uses the process outlined in ISO 31000 risk management guidelines to give guidelines for establishing context and assessing risk, including providing risk scenarios for processes and implementations that are exposed to identity-related risk.
ISO/IEC 27555	Guidelines on personally identifiable information deletion	1st ed. 2021	This document contains guidelines for developing and establishing policies and procedures for deletion of PII in organisations by specifying: • a harmonised terminology for PII deletion, • an approach for defining deletion rules in an efficient way, • a description of required documentation, and • a broad definition of roles, responsibilities and processes.
ISO/IEC 27556	User-centric privacy preferences framework	DIS	ICT systems handling PII should implement privacy control mechanisms with regard to the concept of Privacy-by-Design. In order to implement effective privacy control mechanisms in ICT systems, data handling should be controlled by privacy preferences input by PII principals, including consent information. Therefore, this document provides a user-centric framework for PII handling based on privacy preferences.

Standard	Title	Status	Abstract
ISO/IEC 27557	Organizational privacy risk management	DIS	This document provides guidelines for organizational privacy risk management. It is designed to provide guidance to organizations for integrating risks related to the processing of PII, including the privacy impact to individuals, as part of an organizational privacy risk management program. It also assists in the implementation of a risk-based privacy program which can be integrated in the overall risk management of the organization, and supports the requirement for risk management as specified in management systems (such as ISO/IEC 27701:2019).
ISO/IEC 27559	Privacy enhancing data de-identification framework	DIS	De-identification can be used to strike a balance between protecting personal information and an organizations’ desire to use personal information in new and innovative ways. The appropriate use of de-identification techniques can support compliance with the regulatory requirements and relevant privacy principles. This document provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.

Standard	Title	Status	Abstract
ISO/IEC TS 27560	Consent record information structure	WD	This document specifies an interoperable, open and extensible information structure for recording PII Principals' or data subjects' consent to data processing. It further provides guidance on the use of consent receipts and consent records associated with a PII Principal's data processing consent to support the: • provision of a record of the consent to the PII Principal; • exchange of consent information between information systems; and, • management of the lifecycle of the recorded consent.
ISO/IEC 27561	Privacy operationalisation model and method for engineering (POMME)	CD	This document describes a model and method to operationalize privacy principles into sets of controls and functional capabilities: • The method is described as a process following ISO/IEC/IEEE 24774; • It operationalizes ISO/IEC 29100; • It is intended for engineers and other practitioners developing systems controlling or processing PII; • It is designed for use with other standards and privacy guidance; • It supports networked, interdependent applications and systems.

Standard	Title	Status	Abstract
ISO/IEC 27562	Privacy guidelines for fintech services	WD	This document provides guidelines on privacy for fintech services. It identifies all relevant business models and roles in consumer-to-business relation as well as in business-to-business relation, privacy risks, and privacy requirements, which are related to fintech services. It provides privacy controls specific to fintech services to address the privacy risks, taking in consideration the legal context of the respective business role. The principles are based on the ones described in ISO/IEC 29100, ISO/IEC 27701 and ISO/IEC 29184, and privacy impact assessment framework described in ISO/IEC 29134 and ISO 31000. It also provides guidelines focusing on a set of privacy requirements for each stakeholder.
ISO/IEC TR 27563	Security and privacy in artificial intelligence use cases	DTR	This document provides information on security and privacy in artificial intelligence use cases, covering in particular those published in ISO/IEC TR 24030 (Information technology – Artificial Intelligence (AI) – use cases).
ISO/IEC 27564	Privacy models	PWI	This PWI will study the value of specifying and maintaining privacy models.

Standard	Title	Status	Abstract
ISO/IEC 27565	Guidance on privacy preservation based on zero knowledge proofs	WD	This document provides guidelines on using zero knowledge proofs (ZKP) to improve privacy by reducing the risks associated with the sharing or transmission of personal data between organisations and users by minimizing the information shared. It will include several ZKP functional requirements relevant to a range of different business use cases, then describes how different ZKP models can be used to meet those functional requirements securely.
ISO/IEC TS 27570	Privacy guidelines for smart cities	1st ed. 2021	This document takes a multiple agency as well as a citizen centric viewpoint. It provides guidance on smart city ecosystem privacy protection, on how privacy standards can be used at a global level and at an organizational level for the benefit of citizens, and on processes for smart city ecosystem privacy protection. It is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

Standard	Title	Status	Abstract
ISO/IEC 27701 (developed as ISO/IEC 27552)	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines	1st ed. 2019	ISO/IEC 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and 27002 for privacy management within the context of the organization. It specifies PIMS-related requirements and provides guidance for PII controllers and PII processors. It is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are processing PII within an ISMS.
ISO/IEC TS 29003	Identity proofing	1st ed. 2018 Confirmed 2021	ISO/IEC TS 29003 • 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

Standard	Title	Status	Abstract
ISO/IEC 29101	Privacy architecture framework	2nd ed. 2018	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.
ISO/IEC 29115	Entity authentication assurance framework	1st ed. 2013 Confirmed 2020	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.

Standard	Title	Status	Abstract
ISO/IEC 29134	Guidelines for privacy impact assessment	1st ed. 2017 Amendment in development (DAmd1)	ISO/IEC 29134 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 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.
ISO/IEC 29146	A framework for access management	1st ed. 2016 Confirmed 2020 Amendment in development (DAmd1)	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.

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 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 29184	Online privacy notices and consent	1st ed. 2020	ISO/IEC 29184 specifies controls that shape the content and the structure of online privacy notices as well as the process of asking for consent to collect and process personally identifiable information (PII) from PII principals. This document is applicable in any online context where a PII controller or any other entity processing PII informs PII principals of processing.

Standard	Title	Status	Abstract
ISO/IEC 29190	Privacy capability assessment model	1st ed. 2015 Confirmed 2021	ISO/IEC 29190 provides organizations with guidance how to assess their capability to manage privacy-related processes. In particular, it: • specifies steps in assessing processes to determine privacy capability; • specifies a set of levels for privacy capability assessment; • provides guidance on the key process areas against which privacy capability can be assessed; • provides guidance for those implementing process assessment; and • provides guidance on how to integrate the privacy capability assessment into organizations operations.
ISO/IEC 29191	Requirements for partially anonymous, partially unlinkable authentication	1st ed. 2012 Confirmed 2018	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 PWI 6087	Digital authentication: Risks and mitigations	PWI	
ISO/IEC PWI 6089	Impact of AI on security and privacy	PWI	
ISO/IEC PWI 6102	Guidance on illustrative processes for a privacy information management system	PWI	
ISO/IEC PWI 7732	Age verification	PWI	

Standard	Title	Status	Abstract
Standing Document 1 (SD1)	WG 5 Roadmap		SD 1 gives a graphical and partially textual overview of WG 5 projects and topics not yet covered.
Standing Document 2 (SD2)	Privacy references list	Freely available via www.jtc1sc27.din.de/en	SD2 provides introductory guidance on privacy-related references that have been published to describe data privacy issues and to determine when, how, and to what extent their personally identifiable information should be used, communicated and shared with others.
Standing Document 4 (SD4)	Standards privacy assessment	Freely available via www.jtc1sc27.din.de/en	SD4 defines a Standards Privacy Assessment (SPA) process that provides guidelines for creating a Privacy Considerations section within standards. So this document provides standard and specification editors with guidance on: • Why a Privacy Considerations section is needed in standards and specifications, • When a SPA process should be used for a standard and specification, • How to conduct a SPA analysis on a standard and specification, and • What findings should be included in the Privacy Considerations section of a standard and specification?

SC 27 PROJECTS CONTRIBUTING TO THE UN SUSTAINABLE DEVELOPMENT GOALS

The 2030 UN agenda is an important schedule of international commitment covering seventeen Sustainable Development Goals (SGDs) within the three pillars of development: economic, social and environment).

ISO is helping to meet the United Nations Sustainable Development Goals (SDGs) by maximizing the benefits of international standardization and ensuring the uptake of these standards. Economic, environmental and societal dimensions are all directly addressed by ISO standards. Organizations and companies looking to contribute to the SDGs will find that International Standards provide effective tools to help them rise to the challenge.

For each Goal, ISO has identified the standards that make the most significant contribution, from technical solutions to systems that organize processes and procedures, there are numerous ISO standards that correspond to each of the SDGs. The ISO site https://www.iso.org/sdgs.html serves as a resource for those who are looking for a concrete way in which their organization can play its part.

The table below is a listing of SC 27 projects contributing to the Sustainable Develop Goals (SGDs).

SDG		WG 1	WG 2	WG 4	WG 5
1	NO POVERTY	27001, 27002		27031, 27050-1, 27050-2, 27050-3, 27050-4, 5181, 27099	
2	ZERO HUNGER	27001, 27002		27031, 5181, 27040, 27045, 5689, 7699, 7709, 20547-4, 24392, 27032, 27045, 27400, 27402	
3	GOOD HEALTH AND WELL-BEING	27001, 27002, 27005		27045, 7699, 7709, 20547-4, 27032, 27046	24760, 27570, 29100
4	QUALITY EDUCATION	27021 PWI 27109		27032	24760, 29100, 29190
5	GENDER EQUALITY	27001, 27002, 27005, 27021, PWI 27109		27032	24760, 29100
6	CLEAN WATER AND SANITATION			27400, 27402	
7	AFFORDABLE AND CLEAN ENERGY			27400, 27402, 27403, 27040, 27045, 20547-4, 24392, 27046	24760, 29100, all WG 5 standards
8	DECENT WORK AND ECONOMIC GROWTH	27001, 27002, 27005		27031, 27033-7.2, 27033-1, 27033-2, 27033-3, 27033-4, 27033-5, 27033-6, 27032, 27099, 19086-4	24760, 29100, all WG 5 standards
9	INDUSTRY, INNOVATION AND INFRASTRUCTURE	27001, 27002, 27005, 27006-1, 27010, 27011, 27014, 27017, 27019, 27100, 27110	4922-1, 4922-2.2 14888-4, 18033-7, 29192-8	4983, 24392, 27031, 27040.2, 27046.4, 27402, 27403.5, 27032, 27400, 5181, 27045	24760, 29100, all WG 5 standards
10	REDUCED INEQUALITIES	27001, 27002, 27005, 27014, 27021	20009-3	27035-1, 27035-2, 27035-3, 27035-4, 27037, 27041, 27042, 27043, 27050-1, 27050-2, 27050-3, 27050-4, 5181, 27099, 27032	24760, 29100
11	SUSTAINABLE CITIES AND COMMUNITIES	27001, 27002, 27005, 27006-1, 27010, 27011, 27014, 27017, 27019, 27100, 27110	11770-7, 14888-4 20008-3, 20009-3	4983, 24392, 27031, 27033-7.2, 27046.4, 27402, 27403.5 27045, 27400, 27033-1, 27033-2, 27033-4, 27033-5, 27033-6	24760, 27570, 29100
12	RESPONSIBLE CONSUMPTION AND PRODUCTION	27001, 27002, 27005, 27006-1, 27019	11770-7, 20008-3, 29192-8	4983, 24392, 27035-4, 27040.2, 27046.4, 27402, 27403.5, 27031, 27036-1, 27036-2,	27006-2 27557.2,

				27036-3, 27036-4, 6114, 5689, 27032, 27400	
13	CLIMATE ACTION			27045, 27046, 7699, 7709, 20547-4, 24392, 27400, 27402, 27403	
16	PEACE, JUSTICE AND STRONG INSTITUTIONS	27001, 27002, 27005, 27014		27037, 27041, 27042, 27043, 27050-1, 27050-2, 27050-3, 27050-4, 5181	24760, 29100, all WG 5 standards
17	PARTNERSHIPS FOR THE GOALS	27001, 27006-1, 27007		27032, 27036-1, 27036-2, 27036-3, 27036-4	24760, 29100, all WG 5 standards

1 NO POVERTY (END POVERTY IN ALL ITS FORMS EVERYWHERE)

2 ZERO HUNGER (END HUNGER, ACHIEVE FOOD SECURITY AND IMPROVED NUTRITION AND PROMOTE SUSTAINABLE AGRICULTURE)

3 GOOD HEALTH AND WELL-BEING (ENSURE HEALTHY LIVES AND PROMOTE WELL-BEING FOR ALL AT ALL AGES)

4 QUALITY EDUCATION (ENSURE INCLUSIVE AND EQUITABLE QUALITY EDUCATION AND PROMOTE LIFELONG LEARNING OPPORTUNITIES FOR ALL)

5 GENDER EQUALITY (ACHIEVE GENDER EQUALITY AND EMPOWER ALL WOMEN AND GIRLS)

6 CLEAN WATER AND SANITATION (ENSURE AVAILABILITY AND SUSTAINABLE MANAGEMENT OF WATER AND SANITATION FOR ALL)

7 AFFORDABLE AND CLEAN ENERGY (ENSURE ACCESS TO AFFORDABLE, RELIABLE, SUSTAINABLE AND MODERN ENERGY FOR ALL)

8 DECENT WORK AND ECONOMIC GROWTH (PROMOTE SUSTAINED, INCLUSIVE AND SUSTAINABLE ECONOMIC GROWTH, FULL AND PRODUCTIVE EMPLOYMENT AND DECENT WORK FOR ALL)

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE (BUILD RESILIENT INFRASTRUCTURE, PROMOTE INCLUSIVE AND SUSTAINABLE INDUSTRIALIZATION AND FOSTER INNOVATION)

10 REDUCED INEQUALITIES (REDUCE INEQUALITY WITHIN AND AMONG COUNTRIES)

11 SUSTAINABLE CITIES AND COMMUNITIES (MAKE CITIES AND HUMAN SETTLEMENTS INCLUSIVE, SAFE, RESILIENT AND SUSTAINABLE)

12 RESPONSIBLE CONSUMPTION AND PRODUCTION (ENSURE SUSTAINABLE CONSUMPTION AND PRODUCTION PATTERNS)

13 CLIMATE ACTION (TAKE URGENT ACTION TO COMBAT CLIMATE CHANGE AND ITS IMPACTS)

16 PEACE, JUSTICE AND STRONG INSTITUTIONS (PROMOTE PEACEFUL AND INCLUSIVE SOCIETIES FOR SUSTAINABLE DEVELOPMENT, PROVIDE ACCESS TO JUSTICE FOR ALL AND BUILD EFFECTIVE, ACCOUNTABLE AND INCLUSIVE INSTITUTIONS AT ALL LEVELS)

17 PARTNERSHIPS FOR THE GOALS (Strengthen the means of implementation and revitalize the global partnership for sustainable development)

SC 27 ADVISORY GROUPS

ADVISORY GROUP AG-1 (Management Advisory Group)

- Convenor: Jean-Pierre QUEMARD, AFNOR (FR)

The SC 27 Management Advisory Group (MAG) is an internal administrative function created to review and evaluate the effectiveness of SC27 and make recommendations for improvement. It was created following the 2017 SC 27 Heads of Delegation meeting in Berlin and is composed of ten members plus a Convenor and Vice-Convenor nominated by National Bodies and representing the membership from all SC 27 Working Groups. The MAG normally works electronically, but does in addition hold face-to-face meetings in conjunction with the WG meetings.

The Advisory Group functions purely in an advisory capacity to SC 27 Management. In particular AG 1 does not design any standards. Any recommendations or proposals conveyed to SC 27 Management reflect a consensus outcome among MAG members. The Advisory Group is not empowered to make proposals directly to the SC 27 Plenary, except if granted prior authority by SC 27 Management.

AG1 has been very active in order to propose new ways of working for SC 27. Some of them has been retained by SC 27: Desynchronisation of WG meetings more projects managed in virtual mode, Two plenaries per year. These new ways of working has been put in place in particular because of the COVID pandemic.

ADVISORY GROUP AG-2 (Trustworthiness)

- Convenor: Johann AMSENGA, ILNAS (LU)
- Convenor support; Faud KHAN, SCC (CA)

Since the turn of the century, we have witnessed a significant increase in systems and systems of system complexity where:

- Systems become more IT intensive, as we see for instance with the spread of the Internet of Things (IoT); and, with the convergence of Operational Technologies (OT) and Information Technologies (IT), more cyber in nature;
- Systems become more data intensive, thus the rise of Big Data, and data driven;
- Systems integrate more complex technologies, such as Artificial Intelligence (AI) technologies.

These changes in technologies have enabled the evolution of smart systems and systems of systems such as smart home and buildings, smart grids, smart factories, smart health, precision agriculture, smart transportation and smart cities. These smart systems provide new services that enhance the well-being and the sustainability of our global society. Given the criticality, from both a safety and mission point of view, of these systems, it is necessary to be able to communicate the level of trust in these systems and the services they are providing. Thus, the need for the characterization of the trustworthiness of these systems and their associated enabled services. Trustworthiness can thus contribute to the building of confidence. It is ensured and maintained through a sound governance framework and systems engineering practices. It should be noted that the terms *trust* or *trusted* are sometimes used to characterize specific interactions between technical systems. Systems engaging in such interactions could be considered as trustworthy by operators and users of those systems or by other stakeholders.

SC 27 has established this advisory group to discuss Trustworthiness from a security viewpoint and support the work of JTC 1/WG 13 Trustworthiness. This SC 27 advisory group, through its involvement with the security community, acts as the main contributor on the security aspects of Trustworthiness into JTC 1/WG 13.

ADVISORY GROUP AG-3 (Concepts and Terminology)

- Convenor: Elzbieta ANDRUKIEWICZ, PKN (PL)
- Convenor support: Joanne KNIGHT, NZSO (NZ)

This Advisory Group on Concepts and Terminology is an internal administrative function created to address issues with concepts and terminology across Working Groups, especially where they can affect directly or indirectly multiple WGs.

Alignment of terminology reduces confusion for users of multiple standards and ensures that the clearest language is used in their development. A systematic approach to the development of concepts and terms will makes it easier and faster for new terms to be created and reduce the time spent debating terms. Consistent use and alignment of terminology is also a strong indicator that maturity in the field is being reached.

ADVISORY GROUP AG-5 (Strategy)

- Convenor: Jean-Pierre QUEMARD, AFNOR (FR)

The Advisory Group on Strategy (AG-S) supports the SC 27 Management on strategic issues with respect to upcoming technologies. It shall identify gaps in the portfolio of SC 27 standards and projects to ensure market needs are being adequately addressed, monitor upcoming technologies with respect to their potential relevance of the SC 27 scope, and review issues arising from overlapping or conflicting scopes, activities and projects as well as disagreement on project assignments between Working Groups and beyond, including Committees outside SC 27.

ADVISORY GROUP AG-6 (Operations)

- Convenor: Dr. Qin QIU, SAC (CN);

This advisory group addresses the operational aspects of SC 27: committee functioning of its activities in support of its meetings, work programme, operating procedures and its organization. The group assesses and evaluates all aspects of the operational running of the committee and makes recommendations on operational improvements to SC 27 Management.

ADVISORY GROUP AG-7 (Communications and Outreach)

- Convenor: Dr. Edward HUMPHREYS, BSI (GB);
- Convenor support: Taewan PARK, KATS (KR)

The scope of the communications and outreach activity in SC 27 is to:

- Develop and publish external communications for ISO/IEC JTC 1/SC 27 to complement and supplement information published by ISO;
- Raise awareness about the committee and its work;
- Market published standards as well as ongoing projects;

- Support standards development by promoting this development in communication activities.

The objectives of the communications and outreach aim to:

- Achieve high levels of recognition, support and acceptance of the work of ISO/IEC JTC 1/SC 27 by raising awareness of the committee and its work with the wider stakeholder communities;
- Inform and encourage increased participation of experts in the work of the committee by effective communication of ISO/IEC JTC 1/SC 27 activities and opportunities;
- Increase the use of the standards (and other documents) developed by the committee by increasing public knowledge of their application and value;
- To assist all elements of the ISO/IEC JTC 1/SC 27 community to provide the comprehensive, understandable effective communications internally and externally.

SC 27 JOINT WORKING GROUPS

ISO/IEC JTC 1/SC 27/JWG 6 Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG : Cybersecurity requirements and evaluation activities for connected vehicle devices

- Convenor: Di TANG, SAC, China (appointed by JTC 1/SC 27)
- Co-Convenor: Gido SCHARFENBERGER-FABIAN, DIN, Germany (appointed by JTC 1/TC22/SC32)

The project ISO/IEC NP 5888 has been approved (Information security, cybersecurity and privacy protection - Security requirements and evaluation activities for connected vehicle devices).

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

- Co-Convenor: Julien BRINGER, AFNOR, France (appointed by ISO/TC 307)
- Co-Convenor: Sal FRANCOMACARO, ANSI, USA (appointed by JTC 1/SC 27)

Joint Working Group (JWG) 4 has started its activities in 2018. This JWG is under the administrative responsibility of ISO/TC 307 and JTC 1/SC 27 is the other parent committee. Objective of this JWG is to produce Standards and Technical Reports in the domain of Blockchain Identity, Security and Privacy.

Scope:
This Joint WG was created to leverage different expertise and competences from the two parents' committees to create a synergy among Blockchain experts and Security, Identity and Privacy experts to produce specialized standards in the intersection of the two parent committees while avoiding duplications and possible inconstancies.

Objectives:
The JWG is also working on refining its Programme of Work to answer to the need for standardization in Security, Identity and Privacy for Blockchain. The JWG has a unique capability of collaborating with the working groups of both committees to ensure compatibility with existing standards developed in SC 27 and adaptation to the specificities of blockchain.

Publications

- ISO/TR 23244:2020, Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
- ISO/TR 23576:2020, Blockchain and distributed ledger technologies — Security management of digital asset custodians

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

- ISO/TR 23249 (under publication), Blockchain and distributed ledger technologies - Overview of existing DLT systems for identity management
- ISO/WD TR 23644 (DTR) Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management
- ISO/AWI 7603 (WD) Decentralized Identity standard for the identification of subjects and objects
- ISO/WD TR 23642 (WD) Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues