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

JTC 1/SC 27 Business Plan 2025

Document type	Related content	Document date	Expected action
Project / Other	Meeting: Chengdu (China) 10 Nov 2025	2025-08-06	**COMMENT/REPLY** by 2025-10-13

Description

This document is circulated for review and consideration at the November 2025 JTC 1 Plenary in Chengdu.

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

SC 27 Business Plan 2025

Document type	Related content	Document date	Expected action
General / Other		2025-05-16	**INFO**

Replaces: N 23973 SC 27 Business Plan 2025

ISO/IEC JTC 1/SC 27

Information security, cybersecurity, and privacy protection

Business Plan

Period covered: April 2025 – March 2026

1.0 Executive Summary

Describe the title, scope, and a brief history of the subcommittee. Summarize the markets addressed by the subcommittee, the benefits realized and/or expected from the subcommittee's deliverables and the main objectives or priorities of the subcommittee's work.

SC 27 is an internationally recognized centre of expertise serving the needs of many business sectors and governments. Its work covers both management standards as well as technical standards. SC 27 has brought together many of the world's leading information security, cybersecurity and privacy experts and has so far delivered more than two-hundred and forty-one publications up until January 2024, among them ISO/IEC 27001 and ISO/IEC 27002, two of the most popular standards within ISO. In addition, there are a further seventy-four standards currently under development.

Focusing on the development of generic standards for the protection of information and ICT has led to liaisons with many SDOs and industry bodies, which typically use SC 27 standards as a basis for developing their own discipline and sector-specific security implementation standards.

For SC 27, achieving gender diversity is an important goal across all geographic areas of the world as well as the development of gender responsive standards in line with ISO/IEC JSAG GRS.

As of December 2023, ISO Global Directory lists 1941 experts as committee members, officers or liaison representatives for SC 27 including working groups (duplicates removed).

In December 2022 the composition of the experts listed has been analyzed in more detail. Such analysis will be repeated as soon as access to the necessary data is offered by ISO. It may be assumed that the composition did not significantly change since. 23% of the experts have been female, 77% male. 3% of the SC 27 experts came from Africa, 21% from the Americas, 36% from Asia Pacific and 40% from Europe. One expert from Africa, four experts from the Americas, seven from Asia Pacific, and eleven from Europe worked in SC 27 officer positions. Four out of the twenty-three SC 27 officers were female. Five experts from Africa, forty from America, ninety-two from Asia Pacific, and eighty-four from Europe have been working in SC 27 editor positions. Fifty-two out of the two hundred and twenty-one SC 27 editors and co-editors were female.

2.0 Environment

Explain the overall environment that relates to the scope of the subcommittee, which may include consideration of market dynamics, technology trends, customer/stakeholder needs, competition, existing and potential policies and regulations. This section may include an explanation of how the environment impacts the subcommittee's work.

The current era of digital revolution, including the rapid development of Internet and digital technologies has brought substantial changes in many areas, from our daily life to the processes and methods of industrial production to supporting business transactions and economic developments. This revolution has made the use and application of standardized security techniques a mandatory requirement across almost every sector.

The short-term future sees many market opportunities for SC 27 to expand the deployment of its standards and its expertise as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security, cybersecurity and privacy protection has been at the forefront of standardization in these fields for over thirty years. It has the right mix of skills and resources to deliver security standards to market requirements as demonstrated by its past track record. As applications of security technologies have expanded in recent years, so have both the membership of SC 27 and its programme of work.

The implementation of SC 27 standards can provide confidence, assurance, and trust to stakeholders that cyber risks are being managed and mitigated effectively. This confidence, assurance and trust is established by conformity assessment processes such as system, product, service, and people certifications. Conformity assessment is a demonstration that the specific requirements of SC 27 standards such as ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 15408, ISO/IEC 18405, and ISO/IEC 19896 are being fulfilled and thus providing an independent body written assurance.

In addition, SC 27 is providing its expertise in cybersecurity and privacy protection on emerging technological topics: Artificial Intelligence, Internet of Things and Post Quantum Cryptography. Relying on both its AHG2 IoT and AHG3 AI to ensure coordination between ISO, IEC and JTC 1 SC's. SC 27 is working closely in collaboration with experts from SC 42 (Artificial Intelligence) and SC 41 (Internet of Things) on projects under development like

- ISO/IEC 27090 "Artificial intelligence - Guidance for addressing security threats and failures in artificial intelligence",
- ISO/IEC 27091 "Artificial intelligence – Privacy protection", and
- ISO/IEC 27403 "IoT security and privacy – Guidelines for IoT-domotics"

and has already published several standards related to Internet of Things like

- ISO/IEC 27400:2022 "IoT security and privacy – Guidelines", and
- ISO/IEC 27403 "IoT security and privacy – Device baseline requirements".

3.0 Achievements and benefits

Highlight the subcommittee's achievements and expected benefits of the subcommittee's deliverables to various customers/stakeholders and society overall. Both data and examples would

be helpful to illustrate benefits. Include a summary of the Sustainable Development Goals and ISO and IEC strategies that are directly impacted by the subcommittee's work.

SC 27 is the committee leading the development of standards for information security, cybersecurity, and privacy protection. This includes generic methods, techniques, and guidelines to address both security and privacy aspects, such as:

- Information security, cybersecurity and privacy protection requirements capture methodology;
- Management of information security, cybersecurity, and privacy protection; in particular information security management systems, privacy information management systems, security processes, security controls, services, identity management and privacy technologies;
- 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 and privacy information management systems;
- Security evaluation criteria and methodology.

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

- SDG 3 Good health and well-being;
- SDG 4 Quality education;
- SGD 5 Gender equality;
- SDG 8 Decent work and economic growth;
- SDG 9 Industry, innovation, and infrastructure;
- SDG 10 Reduced inequalities;
- SDG 11 Sustainable cities and communities;
- SDG 12 Responsible consumption and production;
- SDG 13 Climate action; and
- SDG 16 Peace, justice, and strong institutions.

In 2024, SC 27 embarked on the inclusion of requirements on climate actions in its management system standards ISO/IEC 27001 and ISO/IEC 27701. This is in keeping with the TMB directive to comply with ISO policy following the signing of the London Declaration at the ISO General Assembly. Further discussion will be had in SC 27 on the impact of the London Declaration on other standards and the possible need for revised or amended documents.

A full list of the SC 27 projects contributing to the SDGs can be found in the SC 27 committee document CD11 (https://committee.iso.org/home/jtc1sc27) and at the SC 27 Web pages (https://www.iso.org/committee/45306.html).

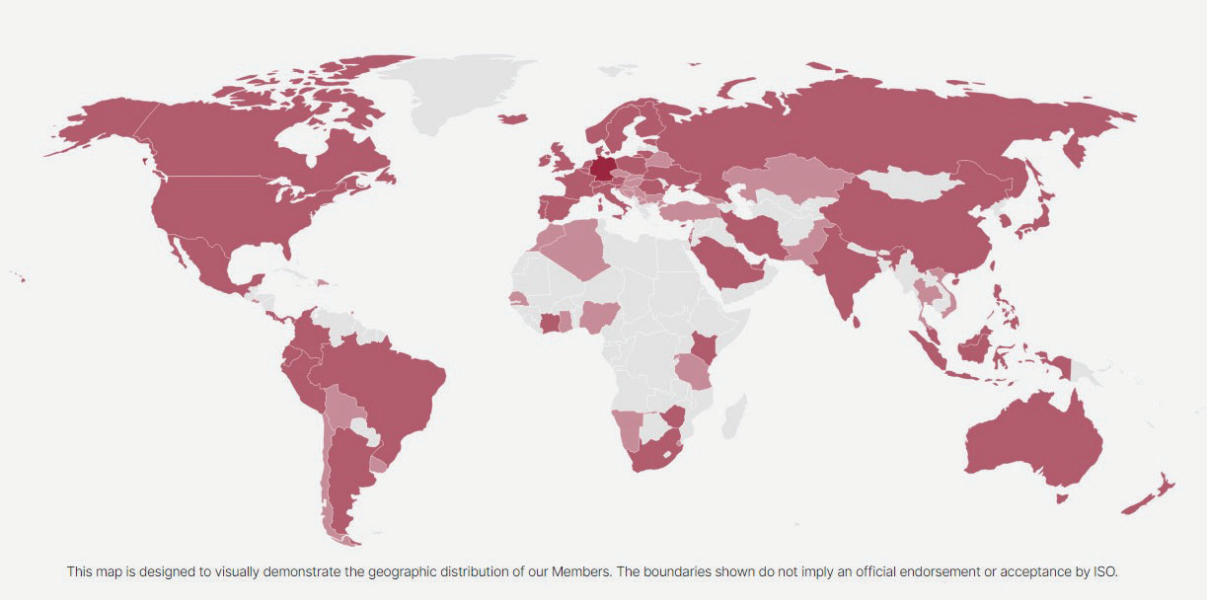
4.0 Participation and cooperation/collaboration.

Note the number of participating and observing members of the subcommittee, indicating any changes since the last plan was published. Include the number of members who participated in at least the last 2 plenary meetings. The section should describe any efforts or plans to increase membership.

List all subcommittee liaison relationships, with other ISO and IEC committees and with external organizations, including consortia. Include comments on specific liaison relationships if desired. Use of a table may be helpful.

Note projects that are being developed through cooperative/collaborative relationships with other ISO and IEC committees, whether via liaison or via Joint Working Groups. This should include projects that are placed in other committees where the subcommittee is making contributions.

Committee membership has increased from eighteen participating members in 1990 to fifty-five participating members (plus thirty-five observing members) in 2024, covering a vast area of the globe.



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

In 2021, the SC 27 Journal, as an additional promotional activity, was launched. The aim is to publish at least three issues of the Journal each year. Every issue contains articles from SC 27 experts that explain the use and application of SC 27 standards. In 2022, SC 27 developed and launched the

committee web site (https://committee.iso.org/home/jtc1sc27/). This is a public website providing an informative overview of SC 27, its working groups and programme of work. This website also gives access to a range of resources and publications such as the SC 27 Journal and the SC 27 committee document CD11, the bi-annual report on the current catalogue of SC 27 standards.

SC 27 has held various workshops, seminars, and conferences to promote their programme of work. These provided an opportunity for SC 27 officers and experts to market and advertise their projects. In late 2024, SC 27 embarked on a number of cybersecurity webinars hosted by the IEC Academy and Capacity Building group in conjunction with ISO. The first of these dealt with ISO/IEC 27001 and Cybersecurity (Nov 2024), followed by a webinar on Cloud Security and IoT Security (Jan 2025). Other webinars in this series are being planned for 2025.

Overall, the level of engagement and expertise is generally sufficient to meet the many challenges SC 27 is facing. For selected projects, SC 27 volunteers are complemented by contributors from appropriate SC 27 liaison organizations.

SC 27 benefits from collaboration with many internal and external liaisons with many committees and organizations. This collaboration is productive and valuable providing many opportunities to ensure the SC 27 standards are complete in their coverage of market requirements. A complete list is available at https://www.iso.org/committee/45306.html, click at Liaisons. Selected aspects related to SC 27 liaisons are highlighted below.

ISO TMB/JTCG (MSS)

ISO TMB/JTCG is involved in all aspects of management system standards (MSS) and the maintenance and future development of ISO Directives Part 1 Annex SL. All work in SC 27 on MSS, such as ISO/IEC 27001 and ISO/IEC 27701, is directly impacted by the activities of JTCG. Also impacted is the family of ISO/IEC 27000 standards some of which are designated as Type B or C MSS documents. SC 27 maintains an active liaison team of experts involved in JTCG.

ISO TMB/JTFRiaT

ISO TMB/JTFRiaT activity has considered the concept of risk and associated terms work across all ISO TC/SCs. The work of this JTF is now complete and its resolutions have been passed to TMB for consideration. SC 27 has been actively involved in this work since risk that is of importance to all SC 27 WGs.

This group has been disbanded as its work is now complete.

IAF

The international accreditation forum is responsible for organizing and coordinating international accreditation. SC 27 is closely involved with IAF because of standards such as ISO/IEC 27001, 27701, ISO/IEC 27006-1 and ISO/IEC 27006-2. IAF is also responsible for the development of transition statements which provides the rules for transitioning from one edition of a standard to the next edition e.g., the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022. IAF are also involved in the SC 27/WG 1 APG (Auditing Practice Group).

JTC 1/SC 37 Biometrics

A close and advantageous synergy exists between biometrics and IT security. The potential contributions of SC 27 to biometrics standards are evident. Particularly, in the areas of template protection techniques, algorithm security, and security evaluation are fields where SC 27 has the necessary experience to complement the mandate of SC 37. Therefore, SC 27 maintains close collaboration with SC 37 Biometrics.

JTC 1/SC 41 Internet of Things

SC 41 is responsible for standardization on Internet of Things and Digital Twin (IoT & DT) and serves as the focus and proponent for JTC 1's standardization programme on that topic. Furthermore, SC 41 provides guidance to JTC 1, IEC, and ISO committees developing IoT & DT applications. Many IoT & DT related standards contain IT security and privacy related components and therefore require close cooperation between SC 27 and SC 41.

In addition, SC 27 has newly established in October 2022 a dedicated ad hoc group AHG2 “Security and privacy in IoT and Digital Twin” which aims to facilitate cooperation within SC 27 WG’s experts on cybersecurity and privacy projects related to internet of things and digital twin as well as the cooperation with SC41 experts and liaisons.

JTC 1/SC 42 Artificial Intelligence

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

In addition, SC 27 has newly established in October 2022 a dedicated ad hoc group AHG3 “Security and privacy in AI and Big Data (BD)” which aims to facilitate cooperation within SC27 WG’s experts on cybersecurity and privacy projects related to artificial intelligence and big data as well as the cooperation with SC 42 experts and liaisons.

ISO/TC 232 Education and learning services

The scope and work of ISO/TC 232, for example ISO 21001:2018 “Educational organizations – Management systems for educational organizations – Requirements with guidance for use”, is of interest to SC 27 and its work on cyber education and training. SC 27 has established liaison with TC 232 to explore areas of common interest.

ISO/TC 292 Security and resilience

ISO/TC 292 is related to many aspects of SC 27 standards work including shared interest in business continuity and ICT readiness, supply chain security and cyber resilience. SC 27 has established a cooperation with TC 292 on topics of common interest with WG 4 “Authenticity, integrity and trust for products and documents” and WG6 “Protective security”. SC 27 also has a particular interest in the following TC 292 projects:

- ISO 22300 series of standards dealing with Security and resilience.
- ISO 28000 series of standards dealing with Security management systems for the supply chain.
- ISO 31050 Risk management – Guidance for managing emerging risks to enhance resilience.

ISO/TC 309 Governance of organizations

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

ISO/TC 307 Blockchain and distributed ledger technologies

ISO/TC 307 was established in 2016 with the goal of standardizing blockchain and distributed ledger technologies. Its scope extends beyond the technologies that underpin blockchain and distributed ledgers to include the generic requirements for their application in sector-specific environments.

Many core technologies utilized by blockchain and distributed ledgers are based on standards already developed by SC 27. To support TC 307's work, SC 27 has established an active liaison relationship. In 2018, SC 27 approved the formation of a joint working group (JWG 4) with TC 307 to enhance expertise and standardization in blockchain security, identity, and privacy. A significant number of SC 27 experts are involved in TC 307 through JWG 4, and this collaboration has proven highly beneficial. Key areas of shared interest for 2025 include decentralized identity, privacy in blockchain systems, and security controls for blockchain systems.

The following JWG 4 projects were published by TC 307:

- ISO/TR 23249:2022 Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management
- ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
- ISO/TR 23644:2023 Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management

The following JWG 4 projects are currently under development:

- ISO 24876 Blockchain and distributed ledger technologies — Privacy protection when involving trust anchors in DLT-based identity management
- ISO 24946 Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems.
- ISO 25126 Information security controls based on ISO/IEC 27002 for distributed ledger services

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

ACSEC deals with information security and data privacy matters which are not specific to any one single IEC technical committee. It coordinates activities related to information security and data privacy and provides advice to IEC/SMB on those subjects. ACSEC provides guidance to TC/SCs for implementation of information security and data privacy in a general perspective and for specific sectors. ACSEC also provides a venue for exchanging information between IEC and other standards developing organizations relevant to ACSEC's scope. ACSEC follows closely both research activities and trends in academia. By participating in ACSEC, SC 27 promotes the application of SC 27 standards in IEC committees and receives updates on standardization needs with respect to IT security from the IEC world. Starting in March 2024, the SC 27 Chair takes over the chair position of ACSEC for three years.

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

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

In 2022, TC 65 and SC 27 created a Joint Advisory Group (JAG 25) to collaborate to avoid and eliminate inconsistencies and gaps in standardization activities in the two committees, and to foster cooperation and information exchange. Overlaps should be minimized and where they occur, standards should ensure that there is a natural flow or link e.g., using references where appropriate, between the standards of one committee to the other.

ITU-T SG 17, SG 13, and ITU-T FG Cloud Computing

ITU-T SG17 and SC 27 collaborate on several projects to progress common or twin text documents and to publish common standards:

- Information security management guidelines for telecommunications (Recommendation ITU -T X.1051 and ISO/IEC 27011:2016)
- Governance of information security (Recommendation ITU-T X.1054 and ISO/IEC 27014:2020)
- Telebiometric authentication framework using biometric hardware security module (Draft Recommendation ITU-T X.1085 and ISO/IEC 17922:2017)
- Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Recommendation ITU-T X.1631 and ISO/IEC 27017:2015)
- Code of practice for the protection of personally identifiable information (Recommendation ITU-T 1058 and ISO/IEC 29151:2017)

Common Criteria Development Board (CCDB)

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

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

Global Privacy Assembly (GPA)

The Global Privacy Assembly first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The GPA has been the premier global forum for data protection and privacy authorities for more than four decades. It seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe. The GPA maintains a Category C liaison with SC 27/ WG 5 helping to be in synch with the global perspective of data protection and privacy authorities, which is also helpful for the adoption of WG 5 standards and the recognition of WG 5. The GPA does not maintain any other liaison to another Standardization organization.

5.0 Objectives and strategies to achieve them

Describe the objectives of the subcommittee - looking to the future and considering future directions. Those objectives may relate to specific projects or groups of projects.

Describe the strategies that the subcommittee has developed to achieve its objectives.

WG1:

ISO/IEC 27001 series – a global phenomenon: The established global market position of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005 as bestselling, flagship ISO/IEC standards in information security management is an outstanding achievement. As well as these standards being classified by ISO as very high profile, a distinction reserved for very few standards, ISO/IEC 27001 is also ranked fourth in the ISO survey of Management System Standards (MSSs). These standards provide a common international language that facilitates many opportunities for growth, trade, and harmonization across all market sectors.

Strategic developments: From a standards perspective WG 1 has strategically developed a critical position on management agendas of organizations across the business spectrum. It is no longer the case of shall we adopt ISO/IEC 27001, it is more the case of can we adopt ISO/IEC 27001 as soon as possible, such is the importance of this standard in managing the risks in today's digital world. The diverse and continual growth in information security and cyber risks and the need for information security and cyberspace governance has made ISO/IEC 27001 central to business strategies and supporting standards such as ISO/IEC 27005, and ISO/IEC 27014 has strengthened this central role for years to come. The work of WG 1 has generated a set of world class horizontal standards with significant outreach for customer and societal demands and requirements, and with benefits for business specific markets. Given the success of the ISO/IEC 27000 series of standards, the WG 1 programme of work attracts the attention of other ISO and IEC TCs/SCs and JTC1 SCs – this presents many opportunities in the application of the ISO/IEC 27000 series of standards across many domains of standardization. By its very nature ISO/IEC 27001 is of strategic importance to IAF (International Accreditation Forum) and the global community of accreditation bodies that support certification services at the national, regional, and international levels.

There has also been significant adoption of ISO/IEC 27001 by governments around the world, as presented in ISO/IEC TR 27024 (Government and regulatory use of ISO/IEC 27001, ISO/IEC 27002 and other information security standards). This TR lists many pieces of national

legislation and regulation where ISO/IEC 27001 and other members of the ISO/IEC 27000 family, are mandatory.

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

ISO/IEC 27001 – Information Security Management Systems – A practical guide for SMEs: In 2024 ISO and IEC has published a practical guide to help Small and Medium Sized Enterprises with the implementation of ISO/IEC 27001. This guide was developed with the assistance of expertise from WG 1. Since its publication it has become a must-have guide by SMEs across many sectors as illustrated by the growth in sales.

ISMS Auditing Practice Group: The ISMS Auditing Practice Group (APG) was launched in 2022 and works in collaboration with IAF and CASCO. The purpose of this group is to develop auditing practice notes (articles) for end users that need help and assistance regarding the requirements of ISO/IEC 27001 and auditing. These are purely for educational and awareness purposes and are not endorsed by ISO or SC 27. This work follows a similar process as adopted by the TC 176 generated 9001 APGs, also in collaboration with IAF and CASCO.

International ISO/IEC 27001 day: WG 1 launched the International 27001 Day on 27 January 2022 to celebrate this successful standard and its high-profile position in the global marketplace. On the 27 January 2023 a second workshop took place to celebrate the release of ISO/IEC 27001:2022 and for conformity assessment bodies to present the global success of ISO/IEC 27001 certification. The International 27002 Day for 2025 will focus on information security and cybersecurity.

WG 2:

WG 2 deals with cryptography and security mechanisms. The group has the task to identify the needs and requirements for these techniques and mechanisms in IT systems and applications and to develop terminology, general models and standards for these techniques and mechanisms for use in security services.

WG 3

In 2022, WG 3 completed the revision of ISO/IEC 15408 and the companion standard ISO/IEC 18045 and has already initiated work to receive feedback from its application by certification schemes, and to investigate the feasibility of further improvements and revision topics. The publication required a fruitful discussion and collaboration between ISO/IEC and the original contributors to this standard, around copyright, and public distribution that can raised some general needs and solutions that could be applicable to other standards.

Standards from WG 3 are increasingly being referred to in legislation and regulations as applied to provide technology assurance in several fields and purposes. In addition to the progressing of the projects under development, current challenges that WG 3 needs to address are related to providing continuous assurance of certified products, and to the security assessment of AI systems.

WG 4

The need for international standards in big data, AI, cybersecurity, secure development, and Internet of Things (IoT) is growing rapidly. As such, more and more projects are being proposed and started in WG 4 in these areas.

WG 4 also continues to work in collaboration with other committees on topics such as big data (JTC 1/SC 7 and JTC 1/SC 42), Internet of Things (JTC 1/SC 25 and JTC 1/SC 41) and AI (JTC 1/SC 42). WG 4 especially involves relevant committees by requesting co-editors and experts from these committees. An example of this is the collaboration with ISO/TC 292, Security, and resilience, on Information and communication technology readiness for business continuity (ISO/IEC 27031). WG 4 also has developed close relationships with its liaisons and will continue to do so in the future. An example is Small Business Standards (SBS) who provided a co-editor for ISO/IEC 27035-1, Information technology – Information security incident management – Part 1: Principles of incident management.

In the coming year, we look to expand our work into the areas such secure development and secure-by-design. This is currently a weak area of coverage for international standards and new collaborations will aid many groups as they are seeking the basis for legislative frameworks globally.

We are starting to see evidence of our standards being referenced in both regulations and legislation for the IoT related projects on the baseline, labeling, and security and privacy controls. We will look to bolster several of our current projects to get the necessary attention to be considered in the future regulations.

WG 5

Privacy and identity management legislation around the world is continuously relying on standards, asking for more standards to implement the respective regulations and for best practices. This is an opportunity, as more and more WG 5 products are receiving attention and are being applied. Moreover, the group is attracting more volunteers. The trend is an opportunity and a challenge, as the group is growing, and the privacy work elsewhere is also intensified. Therefore, WG 5 is continuing to maintain many liaisons. Liaisons with research projects continue to be very successful: Relevant innovative content was contributed, and more volunteers participated in WG 5. At the same time the liaisons with the Global Privacy Assembly (GPA, previously named International Conference of Data Protection and Privacy Commissioners) and the European Data Protection Board (EDPB, successor of the Article 29 Working Party) enable a close relation to regulatory bodies, especially those interpreting and enforcing privacy regulations.

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

The WG 5 experience with virtual only meetings showed that virtual meetings can be arranged easily compared to physical ones. However, their effectiveness is sometimes lower, as they don’t enable

the full spectrum of interaction the standardization process needs, especially in a very interdisciplinary field in a highly contested national and international regulatory environment and for innovative approaches. The positive experience with in-person-meetings after the pandemic in 2022 in Luxembourg continued through the SC 27 WG meetings hosted by the US National Body in Redmond (Washington) in April 2023, a WG 5 meeting in October 2023 in Seoul, Republic of Korea, hosted by the Korean National Body and a further WG 5 meeting in April 2024 in Manchester, hosted by the UK National Body. WG 5 is grateful to NBs inviting for in-person WG meetings and looks forward to the SC 27 WG in-person meetings in March 2025 in the USA and in September 2025 in China and to more invitations for 2026.

JWG 4:

This Joint Working Group (JWG) was established to combine the expertise and competencies of the two parent committees, fostering synergy between blockchain specialists and experts in security, identity, and privacy. The goal is to develop specialized standards at the intersection of these areas while minimizing duplication and potential inconsistencies. Managing a JWG is more complex than overseeing a typical Working Group, which is why two co-convenors have been appointed—one from each committee.

Over the past year, the JWG has experienced growth in both membership and active participation. It is also refining its work programme to address the increasing demand for standardization in blockchain-related security, identity, and privacy. The JWG uniquely collaborates with the working groups of both committees, ensuring alignment with existing SC 27 standards and adapting them to the specific needs of blockchain.

JWG 7:

Given the increasing need for standards related to security testing and evaluation of biometric systems and solutions, this Joint WG was created to leverage different expertise and competences from the two parent committees (SC 27 and SC 37) and to ensure high level of collaboration between experts from the two communities, while avoiding duplications and possible inconstancies. Managing a JWG can be more challenging than a regular WG. For this purpose, two co-convenors have been appointed (one from each committee). This JWG also aims at leveraging synergies with the other WGs of each committee, in particular SC 27/WG 3 on security evaluation and SC 37/WG 5 on biometrics testing.

CAG:

The increasing need for more asynchronous work and more virtual meetings in the future requires more virtualization of decision processes in all committees including SC 27. A platform like CAG can give advice to the chair and the committee manager quickly and on short notice and is able to speed up decisions while increasing their quality.

AG 5:

New technology domains are expanding, and the importance and necessity of cybersecurity is unquestionable. Therefore, the need for international standards in the field of cybersecurity is expected to increase greatly. The group continues to encourage the participation of experts across all fields of JTC 1 and remains open to input and contributions from all relevant international

standardization activities. The Convenor of AG 5 represents SC 27 in the JTC 1/AG 2 Advisory Group on JTC 1 Emerging Technology and Innovation (AG JETI) to identify new domains needing special attention and possible liaison.

AG 6:

Given the circumstances that more and more new experts join SC 27, AG 6 intends to develop reference and introductory materials for them. In the meanwhile, setting encouragement scheme for excellent experts and officers is under study. The SC 27 plenary assigned the maintenance of several SC 27 committee documents to AG 6. With the adoption of the new technology platform and process requirements, AG 6 will review the current SC 27 committee documents and optimize related working recommendations for SC 27.

AG 7:

As the scope and diversity of work in SC 27 continues to grow and expand so does the work of AG 7 to communicate the accomplishments and successes of SC 27 to the global community. Achievements of AG 7 include development and on-going management of the SC 27 website, the publication of the successful SC 27 Journal, the highly acclaimed SC 27 project catalogue in CD11, and other publications. Many further opportunities await AG 7 in the coming years as the SC 27 interface to the outside world extends to embrace new ways of communication and outreach. For example, AG 7 plans to take SC 27 into the world of web-based promotion and social media starting with the launch of the SC 27 hosted Web site (2022). AG 7 has been active on LinkedIn, AG 7 (in conjunction with WG 1) has been involved in the UNIDIR study Gender Approaches to Cybersecurity which considers a range of issues regarding standards for cybersecurity and gender approaches. ISO/IEC 27001 and ISO/IEC 27002 were used as case studies for this UNIDIR activity given the global take-up of these standards by UN members. AG 7 has had a public workshop on Women in Standards – this was a successful event and promoted SC 27 support of the ISO Gender Action Plan and establishment of AG 9 and an SC 27 Diversity officer. The AG 7 Convenor has presented its work at the ISO Standards Day 2023. The convenor also represents SC 27 on JTC 1/AG 1 and AG 10, and has contributed to the JTC 1 Newsletter produced by AG 1.

AG 8:

As the work of SC 27 has continued to grow so has the need for dealing with aspects of conformity assessment (CA) and regular engagement with CASCO. This includes management system certification, people certification and testing and evaluation of products and services. AG 8 acts as a forum for convenors and the SC 27 management to be made aware of conformity assessment issues relating to SC 27 projects, developments regarding CASCO standards, CA advisory notes and use of the SC 27 CA Protocol. The AG 8 Convenor is the SC 27 liaison to CASCO on all matters dealing with conformity assessment.

AG 9:

The advisory group on diversity assists the SC 27 Management team in aligning SC 27 with the ISO and IEC Gender action plan (GAP), helping with enabling ISO and IEC inclusive language policy and gender responsive standards (GRS).

The SC27 GAP 2024-2025 has been developed in coordination with ISO GRSI (gender responsive standards initiative) representatives. Workshops are designed on educating SC 27 members on understanding GRS. Annual reviews and reports on the gender balance of officers and experts, and annual surveys are planned to monitor the GAP.

6.0 Factors affecting completion and adoption of the work programme

Note any factors that could negatively impact completion of key projects or adoption of deliverables.

WG 1:

The universal nature of ISO/IEC 27001 for all information security and cybersecurity management requirements is designed to avoid the non-proliferation of MSS. JTC 1 and SC 27 should protect ISO/IEC 27001 against the risk of the unnecessary proliferation of additional MSS by curbing their development and only endorsing discipline-specific MSS if absolutely justified: Security (ISO/IEC 27001) and privacy (ISO/IEC 27701). The WG 1 Conformity Assessment Advisory Note 1 - Why Is ISO/IEC 27001 Sufficient for the disciplines of Information Security and Cybersecurity? – describes this SC 27 approach.

WG 4:

With consensus process used to develop and product ISO/IEC 27404 and ISO/IEC 27402 these standards are being referenced in more regulations and legislation globally as IoT solutions are expected to hit about 25 billion devices globally next year. Having these standards aid significantly to reduce the overall attack surface of the devices.

7.0 Structure, current projects, and publications

Describe the organizational structure of the subcommittee.

List (or show in an architecture diagram) current projects and indicate the new projects since the last update to the plan. The description may include relevant projects in other committees. Highlight the top few projects that should be given visibility and explain why they are noteworthy or important.

Provide data on the number of publications with a link to the full list. Highlight the top few publications that should be given visibility and explain why they are noteworthy or important.

Note: where requested information is available on a publicly available website, the report may reference a link.

In 2020 and 2021, SC 27 met only in virtual mode, due to the restrictions caused by the COVID-19 pandemic. Starting in April 2020, the virtual meetings went well, SC 27 continuously demonstrated

that virtual meetings of large committees are possible. Starting in 2021, SC 27 changed its meeting mode from one to two plenaries per year.

In 2022, SC 27 scheduled its two plenaries to be virtual and had one larger WG meeting (WG 5) in hybrid mode in September.

In 2023, the April plenary together with WG meetings was face-to-face with some virtual participation, and the October plenary purely virtual. In 2023, SC 27 plenaries were conducted 24/25 April, and 24/25 October.

The April 2024 plenary will be face-to-face (with some virtual participation), with virtual or face-to-face WG meetings scheduled to different locations in the weeks before the plenary. The 2024 April plenary is scheduled for April 16/17/18.

SC 27 expects to have virtual plenaries in the future as well if no host is available. In the future, SC 27 plans to balance the meeting modes and has the intention to schedule one face-to-face and one virtual plenary meeting per year, both lasting for two days.

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

For continuous improvement regarding the efficiency and quality of work and deliverables within SC 27 and its WGs, achieving the right balance between WG autonomy and coordination; and to make optimal use of the relevant processes and tools available, SC 27 has established several Advisory Groups. The SC 27 structure can be viewed at

https://www.iso.org/committee/45306.html

and a list of current projects and publications can be found at

https://www.iso.org/committee/45306/ x/catalogue/p/1/u/0/w/0/d/0.

SC 27 consists of the following Working Groups, Advisory Groups and Ad-hoc Groups:

ISO/IEC JTC 1/SC 27/WG 1 “Information security management systems”

SC 27/WG 1 develops, manages, and maintains the ISO/IEC 27000 family of ISMS standards: management system requirements, supporting codes of practice and implementation guidelines, information security governance, ISMS accreditation, auditing and certification standards, ISMS control standards, competence requirements for ISMS professionals and ISMS applied to cybersecurity. The complete SC 27/WG 1 programme of work can be found described in the SC 27 Committee Document CD11, which is available from the SC 27 public website at https://committee.iso.org/ home/jtc1sc27.

ISO/IEC JTC 1/SC 27/WG 2 “Cryptography and security mechanisms”

The scope of WG 2 covers both cryptographic and non-cryptographic techniques and mechanisms including confidentiality, entity authentication, non-repudiation, key management, and data integrity such as message authentication, hash-functions, and digital signatures.

ISO/IEC JTC 1/SC 27/WG 3 “Security evaluation, testing and specification”

WG 3 covers aspects related to security engineering, with particular emphasis on, but not limited to, standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The areas of interest are 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, and administrative procedures for testing, evaluation, certification, and accreditation schemes.

ISO/IEC JTC 1/SC 27/WG 4 “Security controls and services”

The scope of WG 4 covers aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems. The topics covered include: ICT security operations like readiness, continuity, incident and event management, investigation, information life cycle like creation, processing, storage, transmission and disposal, organizational processes like design, acquisition, development and supply, security aspects of Trusted services like in the provision, operation and management of these services, cloud, internet and cyber security related technologies and architectures like network, virtualization, storage, and digital environments, such as cloud computing, cyber, Internet, and other organizations.

ISO/IEC JTC 1/SC 27/WG 5 “Identity management and privacy technologies”

The scope of SC 27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics, and the protection of personal data. Most important standards are the framework standards ISO/IEC 29100 “Privacy framework” and 24760 “A framework for identity management”, with ISO/IEC 29100 and Part 1 of ISO/IEC 24760 being freely available. Bestsellers are ISO/IEC 27018 “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processorsCode of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”, ISO/IEC 27701 “Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management” and 29134 “Guidelines for privacy impact assessment”. Examples for recent activities are consent records (ISO/IEC 27560), age assurance (ISO/IEC 27566), artificial intelligence (ISO/IEC 27091), avatar interaction in the metaverse (ISO/IEC 27573), and brain-computer interface (BCI) applications (ISO/IEC 27574). The complete SC 27/WG 5 programme of work is described in SC 27 committee document CD11 and in SC 27 committee document CD501 “WG 5 Roadmap”. Both are available from the SC 27 public website at https://committee.iso.org/home/jtc1sc27.

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

JWG 4 commenced its activities in 2018 and operates under the administrative lead of ISO/TC 307 Blockchain and Distributed Ledger Technologies. The aim of this JWG is to develop standards and technical reports in the areas of identity, security, and privacy for Blockchain and DLT systems, drawing on the expertise of both parent committees.

ISO/IEC JTC 1/SC 27 – ISO/IEC JTC 1/SC 37 JWG 7: Cybersecurity testing and evaluation of biometrics

JWG 4 has started its activities late 2024 after approval of the creation by both committees. This JWG is under the administrative responsibility of ISO/IEC JTC 1/SC 27. The objective of this JWG is to

produce standards and reports in the domain of cybersecurity assessment of biometric systems, solutions and technologies, leveraging the expertise of the two parent committees.

ISO/IEC JTC 1/SC 27/AHG 1 “Resolution Drafting”

This AHG is responsible for preparing and drafting resolutions to be presented at plenary meetings.

ISO/IEC JTC 1/SC 27/AHG 2 “Security and privacy in IoT and Digital Twin”

This AHG tracks IoT and Digital Twin security and privacy specific documents and their purpose to avoid duplication and help provide consistency across projects, identifies non IoT and Digital Twin specific documents (published or not) that relate to IoT and Digital Twin and list in what way they relates to them, suggests how SC 27 can address the market need for IoT and Digital Twin security and privacy standards, and creates and maintains a list of existing standards that relates to IoT and Digital Twin security and privacy and in what way and how they are aligned or not.

ISO/IEC JTC 1/SC 27/AHG 3 “Security and privacy in AI and Big Data (BD)”

This AHG tracks AI and BD security and privacy specific documents and their purpose to avoid duplication and help provide consistency across projects, identifies non AI and BD specific documents (published or not) that relate to AI and BD and list in what way they relates to them, suggests how SC 27 can address the market need for AI and BD security and privacy standards, and creates and maintains a list of existing standards that relates to AI and BD security and privacy and in what way and how they are aligned or not.

ISO/IEC JTC 1/SC 27/CAG “Chair’s Advisory Group”

CAG supports the SC 27 chair in leading SC 27 between the plenaries. CAG shall give recommendations to the chair and the committee manager on all decisions which can't be postponed until the next plenary and/or which are unsuitable for a letter ballot. CAG decisions are consensus based. CAG in particular takes part in organizing SC 27 and WG meetings. CAG supports SC 27 liaison representatives handling liaisons to other organizations if necessary or requested.

ISO/IEC JTC 1/SC 27/AG 2 “Trustworthiness”

AG 2 has the task to provide for an environment where SC 27 members can discuss trustworthiness from a security and privacy viewpoint, to act as a single channel from which inputs can be made to JTC 1/WG 13 on trustworthiness, to follow the projects and the terms of reference of the ISO/IEC JTC 1/WG 13 as it is related to SC 27, and to discuss and get consensus on contributions within AG 2 to be made as contributions from SC 27 to JTC 1/WG 13.

ISO/IEC JTC 1/SC 27/AG 5 “Strategy”

AG 5 supports the SC 27 management on strategic issues with respect to upcoming technologies. It shall identify gaps, new opportunities, and strategic move 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 strategic issues arising from overlapping or conflicting scopes, activities, and projects as well as disagreement on project assignments between WGs and beyond, including committees outside SC 27. These proposals will be submitted to SC27 plenary for acceptance. In addition, it will implement an innovative approach on

SC 27 functioning and way of working and coordination between WGs. It will propose to SC 27 management and SC 27 plenary improvement in the processes in respect to JTC 1 rules of conduct. AG 5 shall work with SC 27 WG convenors and members to identify issues like share of work, expertise missing, and responsibilities and to reach acceptable resolutions. AG 5 supports the SC 27 chair and the SC 27 WG convenors and appointed officers to resolve or mitigate potential conflicts whenever such cases are brought to them. The convenor of AG 5 represents SC 27 in the JTC 1 Advisory Group 2 on JTC 1 Emerging Technology and Innovation (AG JETI).

ISO/IEC JTC 1/SC 27/AG 6 “Operations”

The SC 27 Advisory Group on Operations supports the SC 27 management on organizational issues, including aligning and coordinating WG roadmaps and the overall SC 27 roadmap, supporting handling of SC 27 liaisons and common topics with other committees, and maintaining SC 27 committee documents. It was created in 2019 and is composed of the SC 27 management team members, up to 15 representatives of P-Member National Bodies plus a convenor and a convenor support. Currently, the 11 AG 6 NB members come from Argentina, Belgium, China, Germany, Great Britain, Korea, India, Sweden, and Switzerland. AG 6 normally works electronically but holds face-to-face meetings in conjunction with the WG meetings. The Advisory Group functions purely in an advisory capacity to SC 27 management. Any recommendations or proposals conveyed to SC 27 management reflect a consensus outcome among AG 6 members.

ISO/IEC JTC 1/SC 27/AG 7 “Communication and Outreach (AG-CO)”

AG 7 is responsible for all communication and outreach activities related to SC 27, its working groups and advisory groups, and its work programme. The objectives of AG 7 are thus to: achieve high levels of recognition, support and acceptance of the work of SC 27 by raising awareness of the committee and its work with the wider stakeholder communities, develop and publish external communications for SC 27 to complement and supplement information published by ISO, inform and encourage increased participation of experts in the work of the committee by effective communication of SC 27 activities and opportunities, increase the use of the standards (and other documents) developed by the committee by increasing public knowledge of their application and value, and to assist all elements of the SC 27 community to provide the comprehensive, understandable effective communications internally and externally. AG 7 works together with ISO/CS, JTC 1/AG 1 (Communications Advisory Group) and AG 10 (Outreach) and other internal groups involved with communications.

ISO/IEC JTC 1/SC 27/AG 8 “Conformity Assessment”

The purpose of this AG 8 is to support communications and awareness within SC 27 regarding all and every aspect of conformity assessment as it relates to the SC 27 work programme. This includes, but is not limited to, application of SC 27 conformity assessment policy and protocol, reporting of CASCO enquiries and exchanges, reporting of project issues, and SC 27 conformity assessment education and awareness, including conformity assessment advisory notes.

Publications in 2024

ISO/IEC 4922-2:2024	Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing
ISO/IEC TR 5891:2024	Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment
ISO/IEC 9797-2:2021/Cor 1:2024	Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function — Technical Corrigendum 1
ISO/IEC 14888-4:2024	Information security — Digital signatures with appendix — Part 4: Stateful hash-based mechanisms
ISO/IEC 17825:2024	Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
ISO/IEC 18014-2:2021/Cor 1:2024	Information security — Time-stamping services — Part 2: Mechanisms producing independent tokens — Technical Corrigendum 1
ISO/IEC 20008-3:2024	Information security — Anonymous digital signatures — Part 3: Mechanisms using multiple public keys
ISO/IEC 23264-2:2024	Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms
ISO/IEC TS 24462:2024	Information security, cybersecurity and privacy protection — Ontology building blocks for security and risk assessment
ISO/IEC 27001:2022/Amd 1:2024	Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes
ISO/IEC 27006-1:2024	Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General
ISO/IEC 27011:2024	Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 27013:2021/Amd 1:2024	Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 — Amendment 1
ISO/IEC 27019:2024	Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry
ISO/IEC 27035-4:2024	Information technology — Information security incident management — Part 4: Coordination
ISO/IEC 27040:2024	Information technology — Security techniques — Storage security
ISO/IEC 27403:2024	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
ISO/IEC 27554:2024	Information security, cybersecurity and privacy protection — Application of ISO 31000 for assessment of identity-related risk
ISO/IEC 27561:2024	Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)
ISO/IEC 27562:2024	Information technology — Security techniques — Privacy guidelines for fintech services
ISO/IEC 29100:2024	Information technology — Security techniques — Privacy framework

ISO/IEC 29146:2024	Information technology — Security techniques — A framework for access management

Projects under development in 2025

ISO/IEC AWI 4922-3	Information security — Secure multiparty computation — Part 3: Part 3: Mechanisms based on garbled circuits
ISO/IEC CD 5181.2	Information technology — Security and privacy — Data provenance
ISO/IEC AWI TS 5689	Cybersecurity – Security frameworks and use cases for cyber physical systems
ISO/IEC PWI 6109	Guidelines for data security monitoring based on logging
ISO/IEC PWI TS 7709.2	Information technology — Big data security and privacy - Security and privacy-preserving guidelines for multi-sourced data processing
ISO/IEC AWI 9798-5	Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques
ISO/IEC WD 10267	Information technology — Data usage — Personal information factor (PIF) in data related to real persons
ISO/IEC 11770-3:2021/FDAmd 1	Information security — Key management — Part 3: Mechanisms using asymmetric techniques — Amendment 1: TFNS identity-based key agreement
ISO/IEC WD 11770-4	Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets
ISO/IEC CD 11770-8	Information technology — Security techniques — Part 8: Password-based key derivation
ISO/IEC 14888-3:2018/AWI Amd 1	IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms — Amendment 1
ISO/IEC DIS 15408-1	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model
ISO/IEC DIS 15408-2	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components
ISO/IEC DIS 15408-3	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components
ISO/IEC DIS 15408-4	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
ISO/IEC DIS 15408-5	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements
ISO/IEC 18014-1:2008/DAmd 1	Information technology — Security techniques — Time-stamping services — Part 1: Framework — Amendment 1

ISO/IEC PRF 18031	Information technology — Security techniques — Random bit generation
ISO/IEC 18033-2:2006/DAmd 2	Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers — Amendment 2
ISO/IEC 18033-7:2022/AWI Amd 1	Information security — Encryption algorithms — Part 7: Tweakable block ciphers — Amendment 1
ISO/IEC DIS 18045	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation
ISO/IEC PWI 18367	Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing
ISO/IEC PWI 19086-4	Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII
ISO/IEC PWI 19562	Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC FDIS 19790	Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules
ISO/IEC DIS 19792	Information security, cybersecurity and privacy protection — General principles of security evaluation of biometric systems
ISO/IEC DIS 19896-1	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 1: Overview and concepts
ISO/IEC DIS 19896-2	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators
ISO/IEC DIS 19896-3	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 3: Knowledge and skills requirements for ISO/IEC 15408 evaluators and certifiers
ISO/IEC WD 19989-1	Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework
ISO/IEC 20009-4:2017/CD Amd 1	Information technology — Security techniques — Anonymous entity authentication — Part 4: Mechanisms based on weak secrets — Amendment 1
ISO/IEC DTS 20540	Information security, cybersecurity and privacy protection — Testing cryptographic modules in their field
ISO/IEC PWI 22080	Guidance on civil uncrewed aircraft systems (UAS) cybersecurity
ISO/IEC FDIS 24759	Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules
ISO/IEC FDIS 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Core concepts and terminology
ISO/IEC FDIS 24760-2	IT Security and Privacy — A framework for identity management — Part 2: Reference architecture and requirements
ISO/IEC FDIS 24760-3	IT Security and Privacy — A framework for identity management — Part 3: Practice
ISO/IEC WD	IT Security and Privacy — A framework for identity management — Part 4:

24760-4.4	Authenticators, Credentials and Authentication
ISO/IEC PWI 24840	Study and review of authenticate encryption mechanisms for the future revisions of standards
ISO/IEC NP 24843	Information security — Attribute-Based Credentials
ISO/IEC AWI 25093-1	Cybersecurity — Confidential computing — Part 1: Overview and concepts
ISO/IEC PWI 25226	Inclusion of FHE scheme switching techniques in ISO/IEC JTC 1/SC 27/WG 2 standards
ISO/IEC PWI 25227	Inclusion of further attribute-based credential schemes in SC27/WG2 standards
ISO/IEC PWI 25228	Oblivious Transfer Extensions
ISO/IEC PWI 25229	Inclusion of a base oblivious transfer protocol in ISO/IEC JTC 1/SC 27/WG 2 standards
ISO/IEC PWI 25235	Updating SC 27 Committee Document 205 in ISO/IEC JTC 1/SC 27
ISO/IEC PWI 25236	Security notion of FHE
ISO/IEC PWI 25240	Evaluation of AI-based Technology
ISO/IEC PWI 25282	Oblivious Transfer Extensions
ISO/IEC AWI 25330	Information Security — Oblivious Transfer
ISO/IEC PWI 25540	Development of a design specification for the revision of ISO/IEC 27007
ISO/IEC PWI 25541	Algorithmic Mechanisms to Protect Symmetric Algorithms in Hardware Against Side-Channel Attacks
ISO/IEC PWI 25542	Inclusion of digital signature schemes for Post-Quantum Cryptography in ISO/IEC standards
ISO/IEC PWI 25543	Consideration of the Target of Evaluation Concept for Emerging and Existing Technologies (WG3 N2754)
ISO/IEC PWI TR 25544	The effect of different transmission media on the security evaluation of quantum key distribution
ISO/IEC PWI 25545	Guidelines for edge computing security
ISO/IEC PWI 25546	Confidential computing
ISO/IEC PWI 25547	Remedial systems updating
ISO/IEC PWI 25548	Cybersecurity framework for smart cities
ISO/IEC CD 27000	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ISO/IEC AWI 27003	Information technology — Security techniques — Information security management systems — Guidance

ISO/IEC WD 27004	Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
ISO/IEC PWI 27006-1	Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General
ISO/IEC CD TS 27008.2	Information technology — Security techniques — Guidelines for the assessment of information security controls
ISO/IEC DIS 27017	Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC DIS 27018	Information security, cybersecurity and privacy protection – Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC AWI TR 27024	Information security, cybersecurity and privacy protection — Government and regulatory use of ISO/IEC 27001, ISO/IEC 27002 and other information security standards
ISO/IEC DIS 27028	Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes
ISO/IEC 27031	Cybersecurity — Information and communication technology readiness for business continuity
ISO/IEC PWI 27033	Review of 27033
ISO/IEC PWI 27034	Review of 27034
ISO/IEC AWI 27045	Information technology — Big data security and privacy — Guidelines for managing big data risks
ISO/IEC PWI 27046	Information technology — Big data security and privacy — Implementation guidelines
ISO/IEC CD 27090	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems
ISO/IEC WD 27091.2	Cybersecurity and Privacy — Artificial Intelligence — Privacy protection
ISO/IEC CD TS 27103	Information technology — Security techniques — Cybersecurity and ISO and IEC Standards
ISO/IEC AWI TR 27109	Cybersecurity education and training
ISO/IEC WD TS 27115.3	Cybersecurity evaluation of complex systems — Introduction and framework overview
ISO/IEC PWI 27116	Support for customized or multipurpose evaluation
ISO/IEC DIS 27404	Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT
ISO/IEC DIS 27553-2	Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Remote modes
ISO/IEC WD TS 27564	Privacy protection - Guidance on the use of models for privacy engineering
ISO/IEC DIS	Information security, cybersecurity and privacy protection — Guidelines on privacy

27565	preservation based on zero knowledge proofs
ISO/IEC DIS 27566-1	Information technology, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework
ISO/IEC PWI 27566-2	Information technology, cybersecurity and privacy protection — Age assurance systems — Part 2: Technical approaches and guidance for implementation
ISO/IEC WD 27566-3.2	Information technology, cybersecurity and privacy protection — Age assurance systems — Part 3: Benchmarks for benchmarking analysis
ISO/IEC PWI 27568	Security and privacy of digital twins
ISO/IEC PWI TS 27569	Personal identifiable information (PII) processing record information structure
ISO/IEC PWI 27573	Privacy protection of user avatar and system avatar interactions in the metaverse
ISO/IEC PWI 27574	Privacy in brain-computer interface (BCI) applications
ISO/IEC DIS 27701.2	Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance
ISO/IEC FDIS 27706	Information technology, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of privacy information management systems
ISO/IEC CD 28033-1	Information security — Fully homomorphic encryption — Part 1: General
ISO/IEC AWI 28033-2	Fully homomorphic encryption — Part 2: Mechanisms for exact arithmetic on modular integers
ISO/IEC AWI 28033-3	Fully homomorphic encryption — Part 3: Mechanisms for arithmetic on approximate numbers
ISO/IEC CD 28033-4	Information Security - Fully homomorphic encryption — Part 4: Mechanisms for arithmetic based on look-up table evaluation
ISO/IEC NP 28033-5	Fully homomorphic encryption — Part 5: Mechanisms for Scheme Switching
ISO/IEC WD 29115.2	Information security, cybersecurity and privacy protection – Entity authentication assurance framework
ISO/IEC WD 29128-2.2	Information security, cybersecurity and privacy protection — Verification of Cryptographic Protocols — Part 2: Evaluation Methods and Activities for Cryptographic Protocols
ISO/IEC WD 29128-3.2	Information security — Verification of cryptographic protocols — Part 3: Part 3: Evaluation Methods and Activities for Protocol Implementation Verification
ISO/IEC DIS 29151	Information security, cybersecurity and privacy protection – Controls and guidance for personally identifiable information protection
ISO/IEC 29192-1:2012/DAmd 1	Information technology — Security techniques — Lightweight cryptography — Part 1: General — Amendment 1
ISO/IEC 29192-4:2013/WD Amd 2	Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques — Amendment 2
ISO/IEC 29192-8:2022/WD Amd 1	Information security — Lightweight cryptography — Part 8: Authenticated encryption — Amendment 1