S.No	Standard and/or project under the direct responsibility of ISO/IEC JTC 1/SC 27 Secretariat	Scope	WG	Remarks/Indian Experts volunteered to contribute	
1	ISO/IEC CD 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary	This document gives guidance on: -- the standards in the ISO/IEC 27000 family of standards -- the concepts, principles and terminology used in those standards.	WG 1	Dr. Amutha Arunachalam had informed her intention to contribute.	
2	ISO/IEC CD 27017.2 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing: ● additional guidance for relevant controls specified in ISO/IEC 27002: 2022; ● additional controls with guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and guidance for cloud service customers and cloud service providers. This Recommendation | International Standard excludes any and all aspects of conformity assessment.	WG1	Dr. Sanjiv Kumar Agarwala (Oxygen Consulting Services Private Limited), Mr. Sanjeev Chhabra (Wipro) & Mr. N. Sathyan (L& T) had informed their intention to contribute.	

3	ISO/IEC 27019 Information technology — Security techniques — Information security controls for the energy utility industry	This document provides guidance based on ISO/IEC 27002:2022 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.This includes in particular the following: § central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices; § digital controllers and automation components such as control and field devices or Programmable Logic controllers (PLCs), including digital sensor and actuator elements; § all further supporting information systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring,data archiving, historian logging,reporting and documentation purposes; § communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology; § Advanced Metering Infrastructure (AMI) components e.g. smart meters; § measurement devices, e.g. for emission values; § digital protection and safety systems, e.g. protection relays, safety PLCs,emergency governor mechanisms; § energy management systems,e.g. of Distributed Energy Resources (DER), electric charging infrastructures,in private households, residential buildings or industrial customer installations; § distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations; § all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System); § any premises housing the above-mentioned equipment and systems; § remote maintenance systems for above-mentioned systems. This document does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 63096. This document also includes guidance to adapt the risk assessment and treatment processes described in ISO/IEC 27001:2022 to the energy utility industry-sector–specific guidance provided in this document This standard does not involve any aspects of conformity assessment.	WG1	Dr Shalini Bhartiya (Vivekananda Institute of Professional Studies), Mr. N. Sathyan (L&T) & Dr. Sanjiv Kumar Agarwala (Oxygen Consulting Services Private Limited) had informed their intention to contribute.	
4	ISO/IEC CD 27028.2 Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes	This document provides guidance on the use and developing of attributes aligned to ISO/IEC 27002: 2022. Excluded from this standard are aspects of conformity assessment.	WG1		
5	ISO/IEC 27013:2021/PRF Amd 1 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 — Amendment 1		WG 1		

6	ISO/IEC AWI TR 27024 ISO/IEC 27001 family of standards references list — Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements	This technical report contains references to laws, regulations and guidelines relying on International Standards of the ISO/IEC 27001 family. This technical report supports organisations in: a) Identifying the International Standards of the ISO/IEC 27001 family that are recommended or required within the scope of their activities; and b) Developing appropriate information security documentation by benchmarking it with similar practices around the word. This technical report shall not be considered as: • Legal interpretations; and • Having been legally validated by a global law firm or relevant lawyers.	WG 1		
7	ISO/IEC CD TS 27103 Information technology — Security techniques — Cybersecurity and ISO and IEC Standards	This document provides guidance on how to leverage existing standards in a cybersecurity framework.	WG 1		
8	ISO/IEC AWI TR 27109 Cybersecurity education and training	This document provides state of the art information for cyber education and training, useful to those involved in cybersecurity as users, suppliers, certifiers, policy makers and regulators, educationalists, consumers, vendors and manufacturers.	WG 1	Dr. Sanjiv Kumar Agarwala (Oxygen Consulting Services Private Limited) & Mr Tarun Pandey (Meity) had informed their intention to contribute.	
9	ISO/IEC 9797-2:2021/CD Cor 1 Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function — Technical Corrigendum 1		WG 2	Mr Manoj Kumar (Google) had informed his intention to contribute	
10	ISO/IEC 11770-3:2021/DAmd 1 Information security — Key management — Part 3: Mechanisms using asymmetric techniques — Amendment 1: TFNS identity-based key agreement		WG 2	Mr. Shreenivas Hegde (Secure Machine Private Limited), Mr Manoj Kumar (Google) & Dr Gautham Sekar (Madras Fintech Services Private Limited) had informed their intention to contribute	
11	ISO/IEC WD 11770-4 Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets	ISO/IEC 11770-4:2017 defines key establishment mechanisms based on weak secrets, i.e. secrets that can be readily memorized by a human, and hence, secrets that will be chosen from a relatively small set of possibilities. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing offline brute-force attacks associated with the weak secret. ISO/IEC 11770-4:2017 is not applicable to the following aspects of key management: - life-cycle management of weak secrets, strong secrets, and established secret keys; - mechanisms to store, archive, delete, destroy, etc. weak secrets, strong secrets, and established secret keys.	WG 2	Mr. Shreenivas Hegde (Secure Machine Private Limited), Mr Manoj Kumar (Google) & Dr Gautham Sekar (Madras Fintech Services Private Limited) had informed their intention to contribute	
12	ISO/IEC 18014-1:2008/D Amd 1 Information technology — Security techniques — Time-stamping services — Part 1: Framework — Amendment 1		WG 2	Dr. Amutha Arunachalam had informed her intention to contribute.	
13	ISO/IEC 18014-2:2021/Cor 1 Information security — Time-stamping services — Part 2: Mechanisms producing independent tokens — Technical Corrigendum 1		WG 2	Dr. Amutha Arunachalam had informed her intention to contribute.	

14	ISO/IEC PRF 18031 Information technology — Security techniques — Random bit generation	This document specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model. This document specifies the characteristics of the main elements required for both non-deterministic and deterministic random bit generators and establishes the security requirements for both nondeterministic and deterministic random bit generators. The guidelines in Annex B describe how to produce sequences of random numbers from random bit-strings. Techniques for statistical testing of random bit generators for the purposes of independent verification or validation and detailed designs for such generators are outside the scope of this document.	WG 2	Mr. Shreenivas Hegde (Secure Machine Private Limited), Mr Manoj Kumar (Google) & Dr Gautham Sekar (Madras Fintech Services Private Limited) had informed their intention to contribute	
15	ISO/IEC 20009-4:2017/AWI Amd 1 Information technology — Security techniques — Anonymous entity authentication — Part 4: Mechanisms based on weak secrets — Amendment 1		WG 2	Mr Manoj Kumar (Google) had informed his intention to contribute	
16	ISO/IEC 29192-1:2012/D Amd 1 Information technology — Security techniques — Lightweight cryptography — Part 1: General — Amendment 1		WG 2	Mr Manoj Kumar (Google) had informed his intention to contribute	
17	ISO/IEC AWI 11770-8 Information technology — Security techniques — Part 8: Password-based key derivation	This document specifies key derivation functions designed to take human-memorable passwords as input. This document is applicable to environments where it is necessary to derive a cryptographic key from a password. To include the proposed mechanism Argon2 v1.3	WG 2	Dr Gautham Sekar (Madras Fintech Services Private Limited) had informed his intention to contribute	
18	ISO/IEC PWI 24840 Study and review of authenticate encryption mechanisms for the future revisions of standards		WG 2	Mr Manoj Kumar (Google) had informed his intention to contribute	
19	ISO/IEC DIS15408-1 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model	This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.	WG 3	Mr Suresh Chandra (STQC) , Mr Raakesh T (CDAC) & Mr Tarun Pandey (Meity) had informed their intention to contribute	
20	ISO/IEC DIS 15408-2 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components	This document defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.	WG 3	Mr Suresh Chandra (STQC) , Mr Raakesh T (CDAC) & Dr Sumitra Biswal (BOSCH) had informed their intention to contribute	
21	ISO/IEC DIS 15408-3 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components	This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).	WG 3	Mr Suresh Chandra (STQC) & Mr Raakesh T (CDAC) had informed their intention to contribute	
22	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	This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.	WG 3	Mr Suresh Chandra (STQC) & Mr Raakesh T (CDAC) had informed their intention to contribute	
23	ISO/IEC DIS15408-5 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	This document provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders.	WG 3	Mr Suresh Chandra (STQC) & Mr Raakesh T (CDAC) had informed their intention to contribute	
24	ISO/IEC 18033-2:2006/CD Amd 2 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers — Amendment 2		WG 3		

25	ISO/IEC DIS 18045 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation	This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.	WG 3	Mr Suresh Chandra (STQC) had informed his intention to contribute	
26	ISO/IEC DIS 19792 Information security, cybersecurity and privacy protection — General principles of security evaluation of biometric systems	This document provides an overview of the main biometric-specific aspects and specifies principles to be considered for the security evaluation of a biometric system. This document does not address the non-biometric aspects which can form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels). The security evaluation of biometric system conformant to the ISO/IEC 15408 series is out of scope because it is specified in the ISO/IEC 19989 series	WG 3	Mr Suresh Chandra (STQC) had informed his intention to contribute	
27	ISO/IEC DIS 19896-1 Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 1: Introduction, concepts and general requirements	This document provides an overview of the main biometric-specific aspects and specifies principles to be considered for the security evaluation of a biometric system. This document does not address the non-biometric aspects which can form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels). The security evaluation of biometric system conformant to the ISO/IEC 15408 series is out of scope because it is specified in the ISO/IEC 19989 series	WG 3	Mr Raakesh T (CDAC) had informed his intention to contribute	
28	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	This document provides the minimum requirements for the knowledge, skills and effectiveness requirements of assessment body personnel performing testing activities and validating activities for a conformance scheme using ISO/IEC 19790 and ISO/IEC 24759.	WG 3	Mr Raakesh T (CDAC) had informed his intention to contribute	
29	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	This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045.	WG 3	Mr Raakesh T (CDAC) had informed his intention to contribute	
30	ISO/IEC CD TS 20540 Information security, cybersecurity and privacy protection — Testing cryptographic modules in their field	• ISO/IEC 20540 provides recommendations and checklists to support the specification and operational testing of cryptographic modules in their operational environment • The cryptographic modules in ISO/IEC 20540 is validated to ISO/IEC 19790.	WG 3		
31	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	This document defines the evaluation methods and activities to assess the artifacts defined in Part 1 for the verification of the correctness and security of a cryptographic protocol specification using the framework from ISO/IEC 15408-4	WG 3		
32	ISO/IEC WD 29128-3.2 Information security — Verification of cryptographic protocols — Part 3: Part 3: Evaluation Methods and Activities for Protocol Implementation Verification	This document defines the evaluation methods and activities to assess the artifacts defined in Part 1 for the verification of the correctness and security of a cryptographic protocol specification using the framework from ISO/IEC 15408-4	WG 3		

33	ISO/IEC CD 5181 Information technology — Security and privacy — Data provenance	This document provides guidelines, methodology and techniques for deriving securely information manipulating, and transforming data by taking into consideration security and privacy risks occurring during all phases of the life cycle The meta-data derived from data creations and transformations serves for earning trust in entities, stakeholders or processes during the whole lifecycle of data use and data manipulations. By referring to provenance meta-data an information respectively a decision base for data usage is provided to processes and to individuals. Provenance meta-data of data records can also be applied from both, processes, or individuals when they have to decide which one of their data, they want to make voluntarily available to the public as a common good and which one not.	WG 4		
34	ISO/IEC CD 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems	This document provides guidance for organizations to address security threats and failures specific to artificial intelligence (AI) systems. The guidance in this document aims to provide information to organizations to help them better understand the consequences of security threats specific to AI systems, throughout their lifecycle, and descriptions of how to detect and mitigate such threats. This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, that develop or use AI system	WG 4	Mr. Kshitij Bathla (BIS), Dr Sarmistha Neogy (Jadavpur University, Kolkata), Mr Sushil Kumar Nehra (Meity) Mr Yuvaraj Govindarajulu (BOSCH) Mr Suresh Chandra (STQC) & Ms Jyoti Kushwaha (BIS) had informed their intention to contribute	

35	ISO/IEC DIS 27404 Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT	This document defines a Universal Cybersecurity Labelling Framework for the development and implementation of cybersecurity labelling programmes for consumer IoT products and includes guidance on the following topics: • Risks and threats associated with consumer IoT products; • Stakeholders, roles and responsibilities; • Relevant standards and guidance documents; • Conformity assessment options; • Labelling issuance and maintenance requirements; and • Mutual recognition considerations. The scope of this document is limited to consumer IoT products, such as IoT gateways, base stations and hubs to which multiple devices connect; smart cameras, televisions, and speakers; wearable health trackers; connected smoke detectors, door locks and window sensors; connected home automation and alarm systems, especially their gateways and hubs; connected appliances, such as washing machines and fridges; smart home assistants; and connected children's toys and baby monitors. The Universal Cybersecurity Labelling Framework addresses the expected and intended use of IoT devices and systems by consumers, that is, the general public and non-technical users. These devices and systems are used with the understanding that the label and criteria are designed for consumer use and consumer security concerns. Safety is not addressed in this Universal Cybersecurity Labelling Framework even though it is an important aspect to consider. Consumer IoT devices used in an enterprise context may not be classified as consumer IoT devices due to potentially more serious implications if compromised, which then entails more stringent cybersecurity provisions. Furthermore, in threat models of consumer IoT, there is no IT/system administrator as a pre-condition. Products that are not intended for consumer use are excluded from this standard. Examples of excluded devices are those that are primarily intended for manufacturing, healthcare and other industrial purposes. The Universal Cybersecurity Labelling Framework is based on requirements from international standards, with objectives to facilitate mutual recognition of labelling schemes for consumer IoT (regardless if they are binary or multi-level), avoid fragmentation of standards, eradicate duplicated testing (across countries), reduce the cost of compliance and facilitate market access for developers. This document is applicable to consumers, developers, issuing bodies of cybersecurity labels and independent test laboratories.	WG 4	Mr Aseem Jakhar (NuLL),Mr Vishal Kumar (STQC), Mr Suresh Chandra (STQC) & Mr Abhik Chaudhuri (TCS), Dr Vinosh (Qualcom) - had informed their intention to contribute.	
36	PWI 6109 Guidelines for data security monitoring based on logging,		WG 4	Mr. Kshitij Bathla (BIS) & Mr. Raakesh T. (CDAC) had informed their intention to contribute	
37	ISO/IEC DIS 24760-1 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts	This part of ISO/IEC 24760 — 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. This part of ISO/IEC 24760 is applicable to any information system where information relating to identity is processed or stored.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	
38	ISO/IEC DIS 24760-3 Information technology — Security techniques — A framework for identity management — Part 3: Practice	ISO/IEC 24760-3:2016 provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	

39	ISO/IEC WD 24760-4.4 IT Security and Privacy — A framework for identity management — Part 4: Authenticators, Credentials and Authentication	This international standard provides guidance on implementing authentication and the use of credentials therein, in particular it: — describes complementary models for implementing user authentication with different operational aspects; — specifies requirements for the control of identity information transfer in authentication; — specifies formal descriptions of authentication methods; — specifies requirements for authenticators as credentials o managing the lifecycle, o binding to a principal, o use in a federated context.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	
40	ISO/IEC DIS 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	
41	ISO/IEC WD 27091.2 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection	This document provides guidance for organizations to address privacy risks in artificial intelligence (AI) systems and machine learning (ML) models. The guidance in this document helps organizations identify privacy risks throughout the AI system lifecycle, and establishes mechanisms to evaluate the consequences of and treat such risks. This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, that develop or use AI systems.	WG 5	Mr. Kshitij Bathla (BIS), Mr Srinivas P, Mr Sushil Kumar Nehra (Meity), Mr Manoj Kumar (Google) & Dr Shalini Bhartiya (Vivekanand) had earlier informed their intention to contribute	
42	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	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, for storage 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. The preliminary steps for biometric enrolment before authentication procedure are out of scope for this document. The use of biometric identification as part of the authentication procedure is out of scope for this document	WG 5	Dr Vishnu Kanhere (KCPL) & Mr Manoj Kumar (Google) had informed their intention to contribute	
43	ISO/IEC DIS 27565 Guidelines on privacy preservation based on zero knowledge proofs	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 unnecessary information disclosure. It includes 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	WG 5	Mr Srinivas Poosarla (Infosys)- Co-project editor. Mr Manoj Kumar (Google) had informed his intention to contribute	

44	ISO/IEC DIS 27566-1 Information security, cybersecurity and privacy protection — Age assurance systems — Framework — Part 1: Framework	Editor's Note: The scope as per the New Work Item Proposal and balloted on is: This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about the age of, or an agerange for, a natural person. Editor's Note: The ISO/IEC JTC1 SC27 WG5 Experts reviewed the scope statement on 2023-04-18 and considered that it ought to be amended as shown. This will, in due course, require a further P-member ballot, but for now, that is held back pending any other expert comments on scope from the Call for Contributions. Proposed Scope This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about an age threshold of, or an age range for, a natural person.	WG 5	Mr Sushil Kumar Nehra (Meity), Mr Manoj Kumar (Google) & Ms. Jyoti Kushwaha had informed their intention to contribute	
45	ISO/IEC WD 27566-2 Age assurance systems — Part 2: Benchmarks for benchmarking analysis	Editor's Note: The scope as per the New Work Item Proposal and balloted on is: This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about the age of, or an agerange for, a natural person. Editor's Note: The ISO/IEC JTC1 SC27 WG5 Experts reviewed the scope statement on 2023-04-18 and considered that it ought to be amended as shown. This will, in due course, require a further P-member ballot, but for now, that is held back pending any other expert comments on scope from the Call for Contributions. Proposed Scope This document establishes core principles, including privacy, for the purpose of enabling age-related eligibility decisions, by setting out a framework for indicators of confidence about an age threshold of, or an age range for, a natural person.	WG 5	Mr Sushil Kumar Nehra (Meity), Mr Manoj Kumar (Google) & Ms. Jyoti Kushwaha had informed their intention to contribute	
46	ISO/IEC DIS 27701.2 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	This document 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 ISO/IEC 27002 for privacy management within the context of the organization. This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing. This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers or PII processors processing PII within an ISMS	WG 5	Mr Suresh Chandra (STQC) , Ms Jyoti Kushwaha, Mr Manoj Kumar (Google) & Mr Srinivas P (Infosys) had informed their intention to contribute	
47	ISO/IEC DIS 29151 Information technology — Security techniques — Code of practice for personally identifiable information protection	It 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). 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).	WG 5	Mr Suresh Chandra (STQC) & Mr Manoj Kumar (Google) had informed their intention to contribute	
48	ISO/IEC 27574 Privacy in brain-computer interface (BCI) applications	This is India's proposal	WG 5	Mr Srinivas Poosarla (Infosys)- Project editor and Ms Jyoti Kushwaha - Co-editor of this project.	

49	ISO/IEC PWI 27568- Report Security and privacy of digital twins		WG 5	Dr Vishnu Kanhere (KCPL), Mr manoj Kumar (Google) and Mr Srinivas Poosarla (Infosys) - are Co-editor of this project.	
50	ISO/IEC WD TS 27115.2 Cybersecurity evaluation of complex systems — Introduction and framework overview	This document provides the foundations and concepts for the cybersecurity evaluation of complex systems. Two frameworks are defined: • The first is used to specify the cybersecurity of a complex system, including system of systems. • The second is used to evaluate the corresponding cybersecurity solutions.	WG 3		
51	ISO/IEC AWI 4922-3 Information security — Secure multiparty computation — Part 3: Part 3: Mechanisms based on garbled circuit	This document specifies secure multiparty computation mechanisms based on garbled circuit. It describes garbled circuit generation, requirements of input label and garbled circuit evaluation. The mechanisms described in this document include free XOR and half gates.	WG 2		
52	ISO/IEC AWI TS 5689 Security frameworks and use cases for cyber physical systems	This document provides the followings: CPS conceptual model and its specific characteristics – a conceptual model of cyber-physical systems (CPS) and its general features; – specific characteristics of CPS compared to other related concepts; Concerns and security frameworks – security concerns as the basis for the discussion of security risks and security controls for the CPS based on the conceptual model; – several security frameworks to address those security concerns; Practical use cases for CPS – use cases based on the respective security frameworks for CPS; – provision of visibility of use cases into the specific use of the security frameworks, etc. This document does not provide specific security controls needed in cyber-physical systems. This document applies to all sectors where CPS are or will be present, which encapsulate a diverse set of sectors ranging from industrial (e.g., manufacturing) to public (e.g., smart cities). CPS stakeholders such as users, developers, and operators can have a common understanding of CPS (e.g., concepts, risks, security framework) through this document.	WG 4		
53	ISO/IEC AWI 28033-1 Information security — Fully homomorphic encryption — Part 1: General	This document defines the general concepts and principles of fully homomorphic encryption including foundational definitions, symbols and formats. This document also describes the security models, hardness assumptions with concrete security, message spaces, plaintext spaces, ciphertext spaces, and key spaces. Verification that the function itself is computed correctly is outside of the scope.	WG 2		
54	ISO/IEC AWI 28033-2 Information security — Fully homomorphic encryption — Part 2: BGV/BFV variants	This document specifies mechanisms based on BGV (Brakersky-Gentry-Vaikuntanathan) and BFV (Brakerski and Fan-Vercauteren). This document also specifies parameter selection for various security levels.	WG 2		
55	ISO/IEC AWI 28033-3 Information security — Fully homomorphic encryptio — Part 3: CKKS variants	This document specifies mechanisms based on CKKS (Cheon, Kim, Kim, and Song). This document also specifies parameter selection for various security levels.	WG 2		
56	ISO/IEC AWI 28033-4 Information security — Fully homomorphic encryption — Part 4: CGGI variants	This document specifies homomorphic encryption mechanisms for arithmetic based on look-up table evaluation. This document also specifies parameter selection for various security levels.	WG 2		

57	ISO/IEC AWI 9798-5 Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques	ISO/IEC 9798-5:2009 specifies entity authentication mechanisms using zero-knowledge techniques: mechanisms based on identities and providing unilateral authentication; mechanisms based on integer factorization and providing unilateral authentication; mechanisms based on discrete logarithms with respect to numbers that are either prime or composite, and providing unilateral authentication; mechanisms based on asymmetric encryption systems and providing either unilateral authentication, or mutual authentication; mechanisms based on discrete logarithms on elliptic curves and providing unilateral authentication. These mechanisms are constructed using the principles of zero-knowledge techniques, but they are not necessarily zero-knowledge according to the strict definition for every choice of parameters.	WG 2		
58	ISO/IEC 14888-3:2018/AWI Amd 1 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms — Amendment 1		WG 2	Mr Manoj Kumar (Google) had informed his intention to contribute	
59	ISO/IEC WD 19989-1 Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework	For security evaluation of biometric recognition performance and presentation attack detection for biometric verification systems and biometric identification systemsthis document specifies: — extended security functional components to SFR Classes in ISO/IEC 15408-2; — supplementary activities to methodology specified in ISO/IEC 18045 for SAR Classes of ISO/IEC 15408-3. This document introduces the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary activities to methodology, which is additional evaluation activities and guidance/recommendations for an evaluator to handle those activities. The supplementary evaluation activities are developed in this document while the detailed recommendations are developed in ISO/IEC 19989-2 (for biometric recognition aspects) and in ISO/IEC 19989-3 (for presentation attack detection aspects). This document is applicable only to TOEs for single biometric characteristic type. However, the selection of a characteristic from multiple characteristics in SFRs is allowed.	WG 3		
60	ISO/IEC AWI 27003 Information technology — Security techniques — Information security management systems — Guidance	ISO/IEC 27003:2017 provides explanation and guidance on ISO/IEC 27001:2013.	WG 1		

61	ISO/IEC CD TS 27008 Information technology — Security techniques — Guidelines for the assessment of information security controls	This document provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organization's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organization. This document offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001. It is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks.	WG 1		
62	ISO/IEC WD 27566-3.2 Age assurance systems — Part 3: Technical approaches and guidelines for implementation	This document establishes benchmarks for specifying, differentiating and comparing characteristics of age assurance methods and components.	WG 5	Mr Sushil Kumar Nehra (Meity), Mr Manoj Kumar (Google) & Ms. Jyoti Kushwaha had earlier informed their intention to contribute	
63	ISO/IEC DIS 27706.2 Requirements for bodies providing audit and certification of privacy information management systems	This document specifies requirements and provides guidance for bodies providing audit and certification of a privacy information management system (PIMS) according to ISO/IEC 27701 in combination with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 27006-1. The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing PIMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies providing PIMS certification.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	
64	ISO/IEC WD 29115 Information technology — Security techniques — Entity authentication assurance framework	ISO/IEC 29115:2013 provides a framework for managing entity authentication assurance in a given context. In particular, it: - specifies four levels of entity authentication assurance; - specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance; - provides guidance for mapping other authentication assurance schemes to the four LoAs; - provides guidance for exchanging the results of authentication that are based on the four LoAs; and - provides guidance concerning controls that should be used to mitigate authentication threats.	WG 5	Mr Manoj Kumar (Google) had informed his intention to contribute	
65	ISO/IEC AWI 25093-1 Cybersecurity — Confidential computing — Part 1: Overview and concepts	This document provides the overview and concept of confidential computing. This document is applicable for the stakeholders to use confidential computing.	WG 4		
66	ISO/IEC AWI 27045 Information technology — Big data security and privacy — Guidelines for managing big data risks	This document provides guidance on how to navigate the threats that can arise during the big data life cycle from the various big data characteristics that are unique to big data: volume, velocity, variety, variability, volatility, veracity and value.	WG 4		
67	ISO/IEC WD TS 27564 Privacy protection - Guidance on the use of models for privacy engineering	This document provides guidance on how to use modelling in privacy engineering. It describes categories of models that can be used, the use of modelling to support engineering, and the relationships with other references and standards for privacy engineering and for modelling. It provides high-level use cases describing how models are used.	WG 5		

68	ISO/IEC WD 10267 Information technology — Data usage — Personal information factor (PIF) in data related to real persons	This document defines and specifies a standard measure for a ‘Personal Information Factor’ (PIF), which is a result of: • Personal information content of individual data sets or combinations of datasets, • Personal information content of products or services created from individual or combined datasets, for example data sharing, insights or data models, • Individual knowledge of an observer of the datasets, insights or models, • Additional information available to an observer that could be brought to the datasets, insights or models. NOTE: PIF can be used to identify acceptable thresholds for “deidentification” of people centric datasets.	WG 5		
69	ISO/IEC 18033-7:2022/AWI Amd 1 Information security — Encryption algorithms — Part 7: Tweakable block ciphers — Amendment 1		WG 2		
70	ISO/IEC WD 27004 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	ISO/IEC 27004:2016 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 27004:2016 is applicable to all types and sizes of organizations.	WG 1		
71	ISO/IEC 29192-4:2013/WD Amd 2 Information technology — Security techniques — Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques — Amendment 2		WG 2		
72	ISO/IEC 29192-8:2022/WD Amd 1 Information security — Lightweight cryptography — Part 8: Authenticated encryption — Amendment 1		WG 2		