Annex-5

List of JTC 1/SC 27 documents published since 25th meeting of LITD 17

S. no.	Standard & title	Additional information/status of India standard (if published or under print)	Scope	Response Received
1	ISO/IEC 27040:2024 Information technology — Security techniques — Storage security	ISO/IEC 27040 : 2015 has been adopted as IS/ISO/IEC 27040 : 2015	This document provides detailed technical requirements and guidance on how organizations can achieve an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection of data both while stored in information and communications technology (ICT) systems and while in transit across the communication links associated with storage. Storage security includes the security of devices and media, management activities related to the devices and media, applications and services, and controlling or monitoring user activities during the lifetime of devices and media, and after end of use or end of life. Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage products and services, and other non-technical managers or users, in addition to managers and administrators who have specific	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. Likely users of the standard- All organisations developing, integrating or evaluating storage solutions. DigiLocker (https://www.digilocker.gov.in/), Aadhaar Data Vault (https://uidai.gov.in/images/resource/FAQs_Aadhaar_Data_Vault_v1_0_13122017.pdf) This standard is already taken up as LITD/17/25318 IS/ISO/IEC 27040 : 2015 (Identical To: ISO/IEC 27040:2024)- Currently in WC stage.

			responsibilities for information or storage security, storage operation, or who are responsible for an organization’s overall security programme and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security. This document provides an overview of storage security concepts and related definitions. It includes requirements and guidance on the threats, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other international standards and technical reports that address existing practices and techniques that can be applied to storage security.	
2	ISO/IEC 29100:2024 Information technology — Security techniques — Privacy framework	ISO/IEC 29100 : 2011 has been adopted as IS/ISO/IEC 29100 : 2011	This document provides a privacy framework which: — specifies a common privacy terminology; — defines the actors and their roles in processing personally identifiable information (PII); — describes privacy safeguarding considerations; — provides references to known privacy principles for information technology. This document is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where	Mr Srinivas P (Infosys)- I recommend ISO 29100 , the target group being all organizations which come under purview of DPDP Law and it will be useful for companies to use it as guidance document while implementing ISO 27701 or IS 17428 Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. This standard is already taken up as LITD/17/25330 IS/ISO/IEC 29100 : 2011

			privacy controls are required for the processing of PII.	(Identical To: ISO/IEC 29100:2024)- currently in WC stage.
3	ISO/IEC 29146:2024 Information technology — Security techniques — A framework for access management		This document defines and establishes a framework for access management (AM) and the secure management of the process to access information and information and communications technologies (ICT) resources, associated with the accountability of a subject within some contexts. This document provides concepts, terms and definitions applicable to distributed access management techniques in network environments. This document also provides explanations about related architecture, components and management functions. The subjects involved in access management can be uniquely recognized to access information systems, as defined in the ISO/IEC 24760 series. The nature and qualities of physical access control involved in access management systems are outside the scope of this document.	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. Likely users of the standard. - All organisations developing, integrating or evaluating AAA solutions. - National SSO (https://www.meripehchaan.gov.in/)
4	ISO/IEC 17825:2024 Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules		This document specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for security levels 3 and 4. The test metrics are associated with the security functions addressed in ISO/IEC 19790:2012. Testing is conducted at the defined boundary of the cryptographic module and the inputs/outputs	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject.

			available at its defined boundary. This document is intended to be used in conjunction with ISO/IEC 24759:2017 to demonstrate conformance to ISO/IEC 19790:2012. NOTE ISO/IEC 24759:2017 specifies the test methods used by testing laboratories to assess whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012 and the test metrics specified in this document for each of the associated security functions addressed in ISO/IEC 19790:2012. The test approach employed in this document is an efficient “push-button” approach, i.e. the tests are technically sound, repeatable and have moderate costs.	
5	ISO/IEC TS 9569:2023 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045		This document specifies patch management (PAM) security assurance requirements and is intended to be used as an extension of the ISO/IEC 15408 series and ISO/IEC 18045. The security assurance requirements specified in this document do not include evaluation or test activities on the final target of evaluation (TOE), but focus on the initial TOE and on the life cycle processes used by manufacturers. Additionally, this document gives guidance to facilitate the evaluation of the TOE, including the patch and development processes which support the patch management. This document lists options for evaluation authorities (or	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject.

			mutual recognition agreements) on how to utilize the additional assurance and additional evidence in their processes to enable the developer to consistently re-certify their updated or patched TOEs to the benefit of the users. The implementation of these options using an evaluation scheme is out of the scope of this document.	
6	ISO/IEC 20008-2:2013/ Amd 2:2023 Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key — Amendment 2	This is amendment 2 to ISO/IEC 20008-2:2013.		Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject.
7	ISO/IEC 24760-1:2019/ Amd 1:2023 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts — Amendment 1	This is Amendment 1 to ISO/IEC 24760-1:2019		Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. Likely users of the standard. - All organisations developing, integrating or evaluating AAA solutions. - National SSO (https://www.meripehchaan.gov.in/)
8	ISO/IEC 24760-3:2016/ Amd 1:2023 Information technology —	This is Amendment 1 to ISO/IEC 24760-3:2016		Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing,

	Security techniques — A framework for identity management — Part 3: Practice — Amendment 1: Identity Information Lifecycle processes			implementing or evaluating the subject. Likely users of the standard. - All organisations developing, integrating or evaluating AAA solutions. - National SSO (https://www.meripehchaan.gov.in/)
9	ISO/IEC 27033-7:2023 Information technology – Network security — Part 7: Guidelines for network virtualization security	Other Parts of this series has been adopted as IS/ISO/IEC 27033 Part 1, Part 2, Part 3, Part 4, Part 5 & Part 6	This document aims to identify security risks of network virtualization and proposes guidelines for the implementation of network virtualization security. Overall, this document intends to considerably aid the comprehensive definition and implementation of security for any organization’s virtualization environments. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls required to provide secure virtualization environments.	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. Likely users of the standard. - All organisations developing, integrating or evaluating network virtualization.
10	ISO/IEC 27402:2023 Cybersecurity — IoT security and privacy — Device baseline requirements		This document provides baseline ICT requirements for IoT devices to support security and privacy controls.	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. This standard is already taken up as LITD/17/25331 (Identical To: ISO/IEC 27402:2023)- Currently in WC stage.
11	ISO/IEC 29128-1:2023		This document establishes a framework for the verification of cryptographic protocol	Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference

	Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework		specifications according to academic and industry best practices.	to organisation developing, implementing or evaluating the subject.
12	ISO/IEC 27001:2022/Amd 1:2024 Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes	This is Amendment 1 to ISO/IEC 27001:2022		Mr Raakesh. T (CDAC)- I would recommend all standard for India, as they are reference to organisation developing, implementing or evaluating the subject. Likely users of the standard. - All organisations implementing or evaluating security controls based on this international standard. This standard is already taken up as LITD/17/25400 IS/ISO/IEC 27001: 2022- Currently in WC stage.
13	ISO/IEC 4922-2:2024 Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing		This document specifies the processes for secure multiparty computation mechanisms based on the secret sharing techniques which are specified in ISO/IEC 19592-2. Secure multiparty computation based on secret sharing can be used for confidential data processing. Examples of possible applications include collaborative data analytics or machine learning where data are kept secret, secure auctions where each bidding price is hidden, and performing cryptographic operations where the secrecy of the private keys is maintained. This document specifies the mechanisms including but not limited to addition,	

			subtraction, multiplication by a constant, shared random number generation, and multiplication with their parameters and properties. This document describes how to perform a secure function evaluation using these mechanisms and secret sharing techniques.	
14	ISO/IEC TS 24462:2024 Information security, cybersecurity and privacy protection — Ontology building blocks for security and risk assessment		This document defines an inventory of building blocks conceptually associated with different types of assessments of information and communication technology (ICT) trustworthiness. These assessments apply to areas such as governance, risk management, security evaluation, secure development lifecycle (SDL), supply chain integrity and privacy. This document also defines an ontology that organizes these building blocks and provides instructions for using the inventory of building blocks and the ontology. Formalizing the types, categories, and structural characteristics of building blocks in the area of ICT trustworthiness assessment aims to increase efficiency and improve future harmonization in standards development and their use. Building blocks can refer to structural components as well as semantic components. These components can be connected to a variety of concepts and activities related to trustworthiness assessments, including process related, such as traceability or elements of assessment methodologies.	

15	ISO/IEC 27011:2024 Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations	ISO/IEC 27011 : 2016 has been adopted as IS/ISO/IEC 27011 : 2016		This standard is already taken up as LITD/17/25335 IS/ISO/IEC 27011 : 2016 (Identical To: ISO/IEC 27011:2024)- Currently in WC Stage
16	ISO/IEC 27561:2024 Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)		This guidance document describes a model and method to operationalize the privacy principles specified in ISO/IEC 29100 into sets of controls and functional capabilities. The method is described as a process that builds upon ISO/IEC/IEEE 24774. This document is designed for use in conjunction with relevant privacy and security standards and guidance which impact privacy operationalization. It supports networked, interdependent applications and systems. This document is intended for engineers and other practitioners developing systems controlling or processing personally identifiable information.	
17	ISO/IEC TR 5891:2024 Information security, cybersecurity and privacy protection — Hardware monitoring technology for		This document surveys and summarizes the existing hardware monitoring methods, including research efforts and industrial applications. The explored monitoring technologies are classified by applied area, carrier type, target entity, objective pattern, and method of deployment.	

	hardware security assessment		Moreover, this document summarizes the possible ways of utilizing monitoring technologies for hardware security assessment with some existing state-of-the-art security assessment approaches. The hardware mentioned in this document refers only to the core processing hardware, such as the central processing unit (CPU), microcontroller unit (MCU), and system on a chip (SoC), in the von Neumann system and does not include single-input or single-output devices such as memory or displays. The hardware monitoring technology discussed in this document has the following considerations and restrictions: — the monitored target is for the post-silicon phase, not for the design-house phase (e.g. an RTL or netlist design); — monitoring is only applied to the runtime system.	
18	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 27006:2015 has been adopted as IS/ISO/IEC 27006 : 2015	This document specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1. The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing ISMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies providing ISMS certification	