Annex-6

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 14888-4:2024 Information security — Digital signatures with appendix — Part 4: Stateful hash-based mechanisms	Other parts of this series have been adopted as Indian standards as IS/ISO/IEC 14888 Part 1, Part 2 & Part 3.	This document specifies stateful digital signature mechanisms with appendix, where the level of security is determined by the security properties of the underlying hash function. This document also provides requirements for implementing basic state management, which is needed for the secure deployment of the stateful schemes described in this document.	
2.	ISO/IEC 18014-2:2021/Cor 1:2024 Information security — Time-stamping services — Part 2: Mechanisms producing independent tokens — Technical Corrigendum 1	This is Corrigendum 1 to ISO/IEC 18014-2:2021		
3.	ISO/IEC 23264-2:2024 Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms		This document specifies cryptographic mechanisms to redact authentic data. The mechanisms described in this document offer different combinations of the security properties defined and described in ISO/IEC 23264-1. For all mechanisms, this document describes the processes for key generation, generating the	

			redactable attestation, carrying out redactions and verifying redactable attestations. This document contains mechanisms that are based on asymmetric cryptography using three related transformations: — a public transformation defined by a verification key (verification process for verifying a redactable attestation), — a private transformation defined by a private attestation key (redactable attestation process for generating a redactable attestation), and — a third transformation defined by the redaction key (redaction process) allowing to redact authentic information within the constraints set forth during generation of the attestation such that redacted information cannot be reconstructed. This document contains mechanisms which, after a successful redaction, allow the attestation to remain verifiable using the verification transformation and attest that non-redacted fields of the attested message are unmodified. This document further details that the three transformations have the property whereby it is computationally infeasible to derive the private attestation transformation, given the redaction and or the verification transformation and key(s).	

4.	ISO/IEC 27019:2024 Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry	ISO/IEC 27019 : 2017 has been adopted as IS/ISO/IEC 27019 : 2017	This document provides information security controls for the energy utility industry, based on ISO/IEC 27002:2022, 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. for distributed energy resources (DER), electric charging infrastructures, and for 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. distribution management system (DMS) applications or outage management systems (OMS); — 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.	
5.	ISO/IEC 27403:2024 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics		This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT)-domotics systems.	

6.	ISO/IEC 27554:2024 Information security, cybersecurity and privacy protection — Application of ISO 31000 for assessment of identity-related risk		This document provides guidelines for identity-related risk, as an extension of ISO 31000:2018. More specifically, it uses the process outlined in ISO 31000 to guide users in establishing context and assessing risk, including providing risk scenarios for processes and implementations that are exposed to identity-related risk. This document is applicable to the risk assessment of processes and services that rely on or are related to identity. This document does not include aspects of risk related to general issues of delivery, technology or security.	
7.	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	This standard is already taken up as LITD/17/26354 IS/ISO/IEC 27006: 2015 (Identical To: ISO/IEC 27006-1:2024)

8	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.	
9	ISO/IEC 27033-7:2023 Information technology – Network security — Part 7: Guidelines for network virtualization security	Other parts of this series have been adopted as Indian standards 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.	