LIST OF ISO 27002:2022 CONTROLS

Disclaimer: ISO 27002 offers guidelines and best practices for implementing controls and processes defined in ISO 27001.

Domain	Number of controls	Annex	Control	New additions
Organizational	37 controls	5.1	Policies for information security	
		5.2	Information security roles & responsibilities	
		5.3	Segregation of duties	
		5.4	Management responsibilities	
		5.5	Contact with authorities	
		5.6	Contact with special interest groups	
		5.7	Threat intelligence	New
		5.8	Information security in project management	
		5.9	Inventory of information and other associated assets	
		5.10	Acceptable use of information and other associated assets	
		5.11	Return of assets	
		5.12	Classification of information	
		5.13	Labelling of information	
		5.14	Information transfer	
		5.15	Access control	
		5.16	Identity management	
		5.17	Authentication information	

Domain	Number of controls	Annex	Control	New additions
		5.18	Access rights	
		5.19	Information security in supplier relationships	
		5.20	Addressing information security within supplier agreements	
		5.21	Managing information security in the ICT supply chain	
		5.22	Monitoring, review and change management of supplier services	
		5.23	Information security for use of cloud services	New
		5.24	Information security incident management planning and preparation	
		5.25	Assessment and decision on information security events	
		5.26	Response to information security incidents	
		5.27	Learning from information security incidents	
		5.28	Collection of evidence	
		5.29	Information security during disruption	
		5.30	ICT readiness for business continuity	New
		5.31	Legal, statutory, regulatory, and contractual requirements	
		5.32	Intellectual property rights	

Domain	Number of controls	Annex	Control	New additions
		5.33	Protection of records	
		5.34	Privacy and protection of PII	
		5.35	Independent review of information security	
		5.36	Compliance with policies, rules and standards for information security	
		5.37	Documented operating procedures	
People	8 controls	6.1	Screening	
		6.2	Terms & Conditions of Employment	
		6.3	Information security awareness, education and training	
		6.4	Disciplinary process	
		6.5	Responsibilities after termination or change of employment	
		6.6	Confidentiality or non-disclosure agreements	
		6.7	Remote working	
		6.8	Information security event reporting	
Physical	14 controls	7.1	Physical Security Perimeters	
		7.2	Physical entry	
		7.3	Securing offices, rooms and facilities	

Domain	Number of controls	Annex	Control	New additions
		7.4	Physical security monitoring	New
		7.5	Protecting against physical and environmental threats	
		7.6	Working in secure areas	
		7.7	Clear desk and clear screen	
		7.8	Equipment siting and protection	
		7.9	Security of assets off-premises	
		7.10	Storage media	
		7.11	Supporting utilities	
		7.12	Cabling security	
		7.13	Equipment maintenance	
		7.14	Secure disposal or reuse of equipment	
Technological	34 controls	8.1	User endpoint devices	
		8.2	Privileged Access Rights	
		8.3	Information access restriction	
		8.4	Access to source code	
		8.5	Secure authentication	
		8.6	Capacity management	
		8.7	Protection against malware	
		8.8	Management of technical vulnerabilities	

Domain	Number of controls	Annex	Control	New additions
		8.9	Configuration management	New
		8.10	Information deletion	New
		8.11	Data masking	New
		8.12	Data leakage prevention	New
		8.13	Information backup	
		8.14	Redundancy of information processing facilities	
		8.15	Logging	
		8.16	Monitoring activities	New
		8.17	Clock synchronisation	
		8.18	Use of privileged utility programs	
		8.19	Installation of software on operational systems	
		8.20	Networks security	
		8.21	Security of network services	
		8.22	Segregation of networks	
		8.23	Web filtering	New
		8.24	Use of cryptography	
		8.25	Secure development life cycle	
		8.26	Application security requirements	
		8.27	Secure system architecture and engineering principles	

Domain	Number of controls	Annex	Control	New additions
		8.28	Secure coding	New
		8.29	Security testing in development and acceptance	
		8.30	Outsourced development	
		8.31	Separation of development, test and production environments	
		8.32	Change management	
		8.33	Test information	
		8.34	Protection of information systems during audit testing	