

Norm number	Norm title	Implemented	Reason for selection
ISO 27001:2022/A.5			
ISO 27001:2022/A.5.1	Policies for information security	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.2	Information security roles and responsibilities	Yes	Risk and Best Practice, Contractual
ISO 27001:2022/A.5.3	Segregation of duties	Yes	Risk and Best Practice
ISO 27001:2022/A.5.4	Management responsibilities	Yes	Risk and Best Practice
ISO 27001:2022/A.5.5	Contact with authorities	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.6	Contact with special interest groups	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.7	Threat intelligence	Yes	Risk and Best Practice
ISO 27001:2022/A.5.8	Information security in project management	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.9	Inventory of information and other associated assets	Yes	Risk and Best Practice
ISO 27001:2022/A.5.10	Acceptable use of information and other associated assets	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.11	Return of assets	Yes	Risk and Best Practice
ISO 27001:2022/A.5.12	Classification of information	Yes	Risk and Best Practice
ISO 27001:2022/A.5.13	Labeling of information	Yes	Risk and Best Practice
ISO 27001:2022/A.5.14	Information transfer	Yes	Risk and Best Practice
ISO 27001:2022/A.5.15	Access control	Yes	Risk and Best Practice
ISO 27001:2022/A.5.16	Identity management	Yes	Risk and Best Practice
ISO 27001:2022/A.5.17	Authentication information	Yes	Risk and Best Practice
ISO 27001:2022/A.5.18	Access rights	Yes	Risk and Best Practice
ISO 27001:2022/A.5.19	Information security in supplier relationships	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.20	Addressing information security within supplier agreements	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.21	Managing information security in the ICT supply chain	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.22	Monitoring, review, and change management of supplier services	Yes	Risk and Best Practice
ISO 27001:2022/A.5.23	Information security for use of cloud services	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.24	Information security incident management planning and preparation	Yes	Risk and Best Practice
ISO 27001:2022/A.5.25	Assessment and decision on information security events	Yes	Risk and Best Practice
ISO 27001:2022/A.5.26	Response to information security incidents	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.27	Learning from information security incidents	Yes	Risk and Best Practice
ISO 27001:2022/A.5.28	Collection of evidence	Yes	Risk and Best Practice
ISO 27001:2022/A.5.29	Information security during disruption	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.30	ICT readiness for business continuity	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.31	Legal, statutory, regulatory and contractual agreements	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.32	Intellectual property rights	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.5.33	Protection of records	Yes	Risk and Best Practice
ISO 27001:2022/A.5.34	Privacy and protection of PII	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.35	Independent review of information security	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.36	Compliance with policies, rules and standards for information security	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.5.37	Documented operating procedures	Yes	Risk and Best Practice
ISO 27001:2022/A.6			
ISO 27001:2022/A.6.1	Screening	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.6.2	Terms and conditions of employment	Yes	Risk and Best Practice
ISO 27001:2022/A.6.3	Information security awareness, education and training	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.6.4	Disciplinary process	Yes	Risk and Best Practice, Legal / Regulatory Requirement, Contractual Requirement
ISO 27001:2022/A.6.5	Responsibilities after termination or change of employment	Yes	Risk and Best Practice
ISO 27001:2022/A.6.6	Confidentiality or non-disclosure agreements	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.6.7	Remote working	Yes	Risk and Best Practice
ISO 27001:2022/A.6.8	Information security event reporting	Yes	Risk and Best Practice
ISO 27001:2022/A.7			
ISO 27001:2022/A.7.1	Physical security perimeters	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.7.2	Physical entry	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.7.3	Securing offices, rooms and facilities	Yes	Risk and Best Practice, Contractual Requirement
ISO 27001:2022/A.7.4	Physical security monitoring	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.7.6	Working in secure areas	Yes	Risk and Best Practice
ISO 27001:2022/A.7.7	Clear desk and clear screen	Yes	Risk and Best Practice
ISO 27001:2022/A.7.8	Equipment sitting and protection	Yes	Risk and Best Practice
ISO 27001:2022/A.7.9	Security of assets off-premises	Yes	Risk and Best Practice
ISO 27001:2022/A.7.10	Storage media	Yes	Risk and Best Practice
ISO 27001:2022/A.7.11	Supporting utilities	Yes	Risk and Best Practice
ISO 27001:2022/A.7.12	Cabling security	Yes	Risk and Best Practice
ISO 27001:2022/A.7.13	Equipment maintenance	Yes	Risk and Best Practice
ISO 27001:2022/A.7.14	Secure disposal or re-use of equipment	Yes	Risk and Best Practice
ISO 27001:2022/A.8			
ISO 27001:2022/A.8.1	User endpoint devices	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.2	Privileged access rights	Yes	Risk and Best Practice
ISO 27001:2022/A.8.3	Information access rights restrictions	Yes	Risk and Best Practice
ISO 27001:2022/A.8.4	Access to source code	Yes	Risk and Best Practice, Legal / Regulatory Requirement, Contractual Requirement
ISO 27001:2022/A.8.5	Secure authentication	Yes	Risk and Best Practice
ISO 27001:2022/A.8.6	Capacity management	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.7	Protection against malware	Yes	Risk and Best Practice
ISO 27001:2022/A.8.8	Management of technical vulnerabilities	Yes	Risk and Best Practice
ISO 27001:2022/A.8.9	Configuration management	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.10	Information deletion	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.11	Data masking	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.12	Data leakage prevention	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.13	Information backup	Yes	Risk and Best Practice, Legal / Regulatory Requirement, Contractual Requirement
ISO 27001:2022/A.8.14	Redundancy of information processing facilities	Yes	Risk and Best Practice, Legal / Regulatory Requirement, Contractual Requirement
ISO 27001:2022/A.8.15	Logging	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.16	Monitoring activities	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.17	Clock synchronization	Yes	Risk and Best Practice
ISO 27001:2022/A.8.18	Use of privileged utility programs	Yes	Risk and Best Practice
ISO 27001:2022/A.8.19	Installation of software on operational systems	Yes	Risk and Best Practice
ISO 27001:2022/A.8.20	Network security	Yes	Risk and Best Practice
ISO 27001:2022/A.8.21	Security of network services	Yes	Risk and Best Practice, Legal / Regulatory Requirement, Contractual Requirement
ISO 27001:2022/A.8.22	Segregation of networks	Yes	Risk and Best Practice
ISO 27001:2022/A.8.23	Web filtering	Yes	Risk and Best Practice, Legal / Regulatory Requirement
ISO 27001:2022/A.8.24	Use of cryptography	Yes	Risk and Best Practice
ISO 27001:2022/A.8.25	Secure development lifecycle	Yes	Risk and Best Practice
ISO 27001:2022/A.8.26	Application security requirements	Yes	Risk and Best Practice
ISO 27001:2022/A.8.27	Secure system architecture and engineering principles	Yes	Risk and Best Practice
ISO 27001:2022/A.8.28	Secure coding	Yes	Risk and Best Practice
ISO 27001:2022/A.8.29	Security testing in development and acceptance	Yes	Risk and Best Practice
ISO 27001:2022/A.8.30	Outsourced development	Yes	Risk and Best Practice
ISO 27001:2022/A.8.31	Separation of development, test and production environments	Yes	Risk and Best Practice
ISO 27001:2022/A.8.32	Change management	Yes	Risk and Best Practice
ISO 27001:2022/A.8.33	Test information	Yes	Risk and Best Practice
ISO 27001:2022/A.8.34	Protection of information systems during audit testing	Yes	Risk and Best Practice