ISO27002 2022 Controls Table

37 Organisational Controls	8 People Controls	14 Physical Controls	34 Technological Controls
Segregation of duties	Information security awareness, education and training	Securing offices, rooms and facilities	Information access restriction
Management responsibilities	Disciplinary process	Physical security monitoring **(new)**	Access to source code
Contact with authorities	Responsibilities after termination or change of employment	Protecting against physical and environmental threats	Secure authentication
Contact with special interest groups	Confidentiality or non-disclosure agreements	Working in secure areas	Capacity management
Threat intelligence **(new)**	Remote working	Clear desk and clear screen	Protection against malware
Information security in project management	Information security event reporting	Equipment siting and protection	Management of technical vulnerabilities.
Inventory of information and other associated assets		Security of assets off-premises	Configuration management **(new)**
Acceptable use of information and other associated assets		Storage media	Information deletion **(new)**
Return of assets		Supporting utilities	Data masking **(new)**
Classification of information		Cabling security	Data leakage prevention **(new)**
Labelling of information		Equipment maintenance	Information backup
Information transfer		Secure disposal or re-use of equipment	Redundancy of information processing facilities
Access control			Logging

Identity management			Monitoring activities **(new)**
Authentication information			Clock synchronisation
Access rights			Use of privileged utility programs
Information security in supplier relationships			Installation of software on operational systems
Addressing information security within supplier agreements			Networks security
Managing information security in the ICT supply chain			Security of network services
Monitoring, review and change management of supplier services			Segregation of networks
Information security for use of cloud services **(new)**			Web filtering **(new)**
Information security incident management planning and preparation			Use of cryptography
Assessment and decision on information security events			Secure development life cycle
Response to information security incidents			Application security requirements
Learning from information security incidents			Secure system architecture and engineering principles
Collection of evidence			Secure coding **(New)**
Information security during disruption			Security testing in development and acceptance
ICT readiness for business continuity **(new)**			Outsourced development
Legal, statutory, regulatory, and contractual requirements			Separation of development, test and production environments

Intellectual property rights			Change management
Protection of records			Test information
Privacy and protection of PII			Protection of information systems during audit testing
Independent review of information security			
Compliance with policies, rules and standards for information security			
Documented operating procedures			