Blackmores

ISO 27001:2022 Annex A Controls Mapping

ISO 27001:2022 Control Group Key:

🟦	A.5 Organisational (37 Controls)
🟩	A.6 People (8 Controls)
🟥	A.7 Physical (14 Controls)
🟨	A.8 Technological (34 Controls)

ISO 27001:2013 Information technology: Security Techniques - ISMS Requirements		ISO 27001:2022 Information security, cybersecurity and privacy protection - ISMS Requirements	
Control Ref	Title	Control Ref	Title
A.5	**Information Security Policies.**		
A.5.1.1	Policies for information security	A.5.1	Policies for information security
A.5.1.2	Review of policies for Information security	A.5.1	Policies for information security
A.6	**Organization of information security**		
A.6.1.1	Information Security roles and responsibilities	A.5.2	Information security roles and responsibilities
A.6.1.2	Segregation of duties	A.5.3	Segregation of duties
A.6.1.3	Contact with authorities	A.5.5	Contact with authorities
A.6.1.4	Contact with special interest groups	A.5.6	Contact with special interest groups
A.6.1.5	Information security in project management	A.5.8	Information security in project management
A.6.2.1	Mobile device policy	A.8.1	User end point devices
A.6.2.2	Teleworking	A.6.7	Remote working
A.7	**Human resource security**		
A.7.1.1	Screening	A.6.1	Screening
A.7.1.2	Terms and conditions of employment	A.6.2	Terms and conditions of employment
A.7.2.1	Management Responsibilities	A.5.4	Management responsibilities
A.7.2.2	Information security awareness, education and training	A.6.3	Information security awareness, education and training
A.7.2.3	Disciplinary process	A.6.4	Disciplinary process
A.7.3.1	Termination or change of employment responsibilities	A.6.5	Responsibilities after termination or change of employment
A.8	**Asset Management**		
A.8.1.1	Inventory of assets	A.5.9	Inventory of information and other associated assets
A.8.1.2	Ownership of assets	A.5.9	Inventory of information and other associated assets
A.8.1.3	Acceptable use of assets	A.5.10	Acceptable use of information and other associated assets
A.8.1.4	Return of assets	A.5.11	Return of assets
A.8.2.1	Classification of information	A.5.12	Classification of information
A.8.2.2	Labelling of information	A.5.13	Labelling of information
A.8.2.3	Handling of assets	A.5.10	Acceptable use of information and other associated assets
A.8.3.1	Management of removable media	A.7.10	Storage media
A.8.3.2	Disposal of Media	A.7.10	Storage media
A.8.3.3	Physical media transfer	A.7.10	Storage media
A.9	**Access Control**		
A.9.1.1	Access control policy	A.5.15	Access control
A.9.1.2	Access to networks and network services	A.5.15	Access control
A.9.2.1	User registration and de-registration	A.5.16	Identity management
A.9.2.2	User access provisioning	A.5.18	Access rights
A.9.2.3	Management of privileged access rights	A.8.2	Privileged access rights
A.9.2.4	Management of secret authentication information users	A.5.17	Authentication information
A.9.2.5	Review of user access rights	A.5.18	Access rights
A.9.2.6	Removal or adjustment of access rights	A.5.18	Access rights
A.9.3.1	Use of secret authentication information	A.5.17	Authentication information
A.9.4.1	Information access restriction	A.8.3	Information access restrictions
A.9.4.2	Secure log on Procedures	A.8.5	Secure authentication
A.9.4.3	Password Management system	A.5.17	Authentication information
A.9.4.4	Use of privileged utility programs	A.8.18	Use of privileged utility programs
A.9.4.5	Access control to program source code	A.8.4	Access to source code
A.10	**Cryptography**		
A.10.1.1	Policy on the use of cryptographic controls	A.8.24	Use of cryptography
A.10.1.2	Key Management	A.8.24	Use of cryptography
A.11	**Physical and environmental security**		
A.11.1.1	Physical security perimeter	A.7.1	Physical security perimeters
A.11.1.2	Physical entry controls	A.7.2	Physical entry
A.11.1.3	Securing offices, rooms and facilities	A.7.3	Securing offices, rooms and facilities
A.11.1.4	Protecting against external and environmental threats	A.7.5	Protecting against physical and environmental threats
A.11.1.5	Working in secure areas	A.7.6	Working in secure areas
A.11.1.6	Delivery and loading areas	A.7.2	Physical entry
A.11.2.1	Equipment siting and protection	A.7.8	Equipment siting and protection
A.11.2.2	Supporting utilities	A.7.11	Supporting utilities
A.11.2.3	Cabling security	A.7.12	Cabling security
A.11.2.4	Equipment maintenance	A.7.13	Equipment maintenance
A.11.2.5	Removal of assets	A.7.10	Storage media
A.11.2.6	Security of equipment and assets of off premises	A.7.9	Security of assets off-premises
A.11.2.7	Secure disposal or re-use of equipment	A.7.14	Secure disposal or re-use of equipment
A.11.2.8	Unattended user equipment	A.8.1	User end point devices
A.11.2.9	Clear Desk and Clear Screen Policy	A.7.7	Clear desk and clear screen
A.12	**Operations security**		
A.12.1.1	Documented operating procedures	A.5.37	Documented operating procedures
A.12.1.2	Change management	A.8.32	Change management
A.12.1.3	Capacity management	A.8.6	Capacity management
A.12.1.4	Separation of development, testing and operational environments	A.8.31	Separation of development, test and production environments
A.12.2.1	Control against malware	A.8.7	Protection against malware
A.12.3.1	Information backup	A.8.13	Information backup
A.12.4.1	Event logging	A.8.15	Logging
A.12.4.2	Protection of log information	A.8.15	Logging
A.12.4.3	Administrator and operator logs	A.8.15	Logging
A.12.4.4	Clock synchronisation	A.8.17	Clock synchronisation
A.12.5.1	Installation of software on operational systems	A.8.19	Installation of software on operational systems
A.12.6.1	Management of technical vulnerabilities	A.8.8	Management of technical vulnerabilities
A.12.6.2	Restrictions on software installation	A.8.19	Installation of software on operational systems
A.12.7.1	Information systems audit controls	A.8.34	Protection of information systems during audit testing
A.13	**Communications security**		
A.13.1.1	Network controls	A.8.20	Networks security
A.13.1.2	Security of network services	A.8.21	Security of network services
A.13.1.3	Segregation in networks	A.8.22	Segregation of networks
A.13.2.1	Information transfer policies and procedures	A.5.14	Information transfer
A.13.2.2	Agreements on information transfer	A.5.14	Information transfer
A.13.2.3	Electronic messaging	A.5.14	Information transfer
A.13.2.4	Confidentiality or non disclosure agreements	A.6.6	Confidentiality or non disclosure agreements
A.14	**System acquisition, development and maintenance**		
A.14.1.1	Information security requirements analysis and specification	A.5.8	Information security in project management
A.14.1.2	Securing application services on public networks	A.8.26	Application security requirements
A.14.1.3	Protecting application services and transactions	A.8.26	Application security requirements
A.14.2.1	Secure development policy	A.8.25	Secure development life-cycle
A.14.2.2	System change control procedures	A.8.32	Change management
A.14.2.3	Technical review of applications after Operating platform changes	A.8.32	Change management
A.14.2.4	Restrictions on changes to software packages	A.8.32	Change management
A.14.2.5	Secure system engineering principles	A.8.27	Secure system architecture and engineering principles
A.14.2.6	Secure development environment	A.8.31	Separation of development, test and production environments
A.14.2.7	Outsourced development	A.8.30	Outsourced development
A.14.2.8	System security testing	A.8.29	Security testing in development and acceptance
A.14.2.9	System acceptance testing	A.8.29	Security testing in development and acceptance
A.14.3.1	Protection of test data	A.8.33	Test information
A.15	**Supplier relationships**		
A.15.1.1	Information security policy for supplier relationships	A.5.19	Information security in supplier relationships
A.15.1.2	Addressing security within supplier agreements	A.5.20	Addressing information security within supplier agreements
A.15.1.3	Information and communication technology supply chain	A.5.21	Managing information security in the information and communication technology (ICT) supply chain
A.15.2.1	Monitoring and review of supplier services	A.5.22	Monitoring, review and change management of supplier services
A.15.2.2	Managing changes to supplier services	A.5.22	Monitoring, review and change management of supplier services
A.16	**Information security incident management**		
A.16.1.1	Responsibilities and Procedures	A.5.24	Information security incident management planning and preparation
A.16.1.2	Reporting information security events	A.6.8	Information security event reporting
A.16.1.3	Reporting information security weaknesses	A.6.8	Information security event reporting
A.16.1.4	Assessment of and decision on information security events	A.5.25	Assessment and decision on information security events
A.16.1.5	Response to information security incidents	A.5.26	Response to information security incidents
A.16.1.6	Learning from Information security incidents	A.5.27	Learning from information security incidents
A.16.1.7	Collection of evidence	A.5.28	Collection of evidence
A.17	**Information security aspects of business continuity management**		
A.17.1.1	Planning information security continuity	A.5.29	Information security during disruption
A.17.1.2	Implementation information security continuity.	A.5.29	Information security during disruption
A.17.1.3	Verify, review and evaluate information security continuity	A.5.29	Information security during disruption
A.17.2.1	Availability of information processing facilities	A.8.14	Redundancy of information processing facilities
A.18	**Compliance**		
A.18.1.1	Identification of applicable legislations and contractual requirements	A.5.31	Legal, statutory, regulatory and contractual requirements
A.18.1.2	Intellectual Property Rights (IPR)	A.5.32	Intellectual property rights
A.18.1.3	Protection of records	A.5.33	Protection of records
A.18.1.4	Privacy and protection of personally identifiable information	A.5.34	Privacy and protection of personally identifiable information (PII)
A.18.1.5	Regulation of cryptographic controls	A.5.31	Legal, statutory, regulatory and contractual requirements
A.18.2.1	Independent review of information security	A.5.35	Independent review of information security
A.18.2.2	Compliance with security policies and standards	A.5.36	Compliance with policies, rules and standards for information security
A.18.2.3	Technical compliance review	A.5.36 A.8.8	Compliance with policies, rules and standards for information security Management of technical vulnerabilities
			ISO27001:2022 New controls
		A.5.7	Threat intelligence
		A.5.23	Information security for use of cloud services
		A.5.30	ICT readiness for business continuity
		A.7.4	Physical security monitoring
		A.8.9	Configuration management
		A.8.10	Information deletion
		A.8.11	Data masking
		A.8.12	Data leakage prevention
		A.8.16	Monitoring activities
		A.8.23	Web filtering
		A.8.28	Secure coding

www.blackmoresuk.com ☎ +44 (0) 1462 514549 ✉ enquiries@blackmoresuk.com