

# Ark - ISO27001 Statement of Applicability (SOA) - External

Version:	5.0	Document ID:	14127-I-ISO27001 SOA	Issue Date:	16/04/2024
Document Owner:	Lucy Pryke	Ark Public		Document Approver:	Louise Methven
Section	Control Reference	Section Heading	Control	Applicable	
Organisational Controls (5)	5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	
Organisational Controls (5)	5.2	Information security roles & responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Yes	
Organisational Controls (5)	5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes	
Organisational Controls (5)	5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	
Organisational Controls (5)	5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Yes	
Organisational Controls (5)	5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	
Organisational Controls (5)	5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Yes	
Organisational Controls (5)	5.8	Information security in project management	Information security should be integrated into project management.	Yes	
Organisational Controls (5)	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes	
Organisational Controls (5)	5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes	
Organisational Controls (5)	5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	
Organisational Controls (5)	5.12	Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	
Organisational Controls (5)	5.13	Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	
Organisational Controls (5)	5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	
Organisational Controls (5)	5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Yes	
Organisational Controls (5)	5.16	Identity management	The full life cycle of identities should be managed.	Yes	
Organisational Controls (5)	5.17	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	
Organisational Controls (5)	5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	
Organisational Controls (5)	5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	
Organisational Controls (5)	5.2	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	
Organisational Controls (5)	5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	
Organisational Controls (5)	5.22	Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	
Organisational Controls (5)	5.23	Information Security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Yes	
Organisational Controls (5)	5.24	Information Security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	
Organisational Controls (5)	5.25	Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Yes	
Organisational Controls (5)	5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Yes	
Organisational Controls (5)	5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Yes	
Organisational Controls (5)	5.28	Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	
Organisational Controls (5)	5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes	
Organisational Controls (5)	5.3	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	

Organisational Controls (5)	5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	Yes
Organisational Controls (5)	5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	Yes
Organisational Controls (5)	5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes
Organisational Controls (5)	5.34	Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes
Organisational Controls (5)	5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes
Organisational Controls (5)	5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Yes
Organisational Controls (5)	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes
People Controls (6)	6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes
People Controls (6)	6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Yes
People Controls (6)	6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes
People Controls (6)	6.4	Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes
People Controls (6)	6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Yes
People Controls (6)	6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes
People Controls (6)	6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes
People Controls (6)	6.8	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes
Physical Controls (7)	7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes
Physical Controls (7)	7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Yes
Physical Controls (7)	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Yes
Physical Controls (7)	7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	Yes
Physical Controls (7)	7.5	Protecting against physical and environmental threats	To prevent or reduce the consequences of events originating from physical and environmental threats.	Yes
Physical Controls (7)	7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Yes
Physical Controls (7)	7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes
Physical Controls (7)	7.8	Equipment siting and protection	Equipment should be sited securely and protected.	Yes
Physical Controls (7)	7.9	Security of assets off-premises	Off-site assets should be protected.	Yes
Physical Controls (7)	7.1	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes
Physical Controls (7)	7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes
Physical Controls (7)	7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Yes
Physical Controls (7)	7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes
Physical Controls (7)	7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes
Technological Controls (8)	8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes
Technological Controls (8)	8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Yes
Technological Controls (8)	8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes
Technological Controls (8)	8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes
Technological Controls (8)	8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes
Technological Controls (8)	8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes
Technological Controls (8)	8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Yes

Technological Controls (8)	8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes
Technological Controls (8)	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes
Technological Controls (8)	8.1	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Yes
Technological Controls (8)	8.11	Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes
Technological Controls (8)	8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes
Technological Controls (8)	8.13	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes
Technological Controls (8)	8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes
Technological Controls (8)	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes
Technological Controls (8)	8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes
Technological Controls (8)	8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes
Technological Controls (8)	8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes
Technological Controls (8)	8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes
Technological Controls (8)	8.2	Network security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes
Technological Controls (8)	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes
Technological Controls (8)	8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.	Yes
Technological Controls (8)	8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Yes
Technological Controls (8)	8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes
Technological Controls (8)	8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	Yes
Technological Controls (8)	8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes
Technological Controls (8)	8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes
Technological Controls (8)	8.28	Secure coding	Secure coding principles should be applied to software development.	Yes
Technological Controls (8)	8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Yes
Technological Controls (8)	8.3	Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Yes
Technological Controls (8)	8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Yes
Technological Controls (8)	8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes
Technological Controls (8)	8.33	Test information	Test information should be appropriately selected, protected and managed.	Yes
Technological Controls (8)	8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes