esri UK & Ireland
THE SCIENCE OF WHERE

Esri UK and Esri Ireland: ISO 27001:2022 SoA v1 - March 2024

Applicability	Activity reference	Control / Activity	Objective / Deliverable	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
Applicable - implemented	A.5.1	Policies for information security	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Governance	Governance and Ecosystem, Resilience
Applicable - implemented	A.5.2	Information security roles and responsibilities	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Governance	Governance and Ecosystem, Protection, Resilience
Applicable - implemented	A.5.3	Segregation of duties	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Governance, Identity and access management	Governance and Ecosystem
Applicable - implemented	A.5.4	Management responsibilities	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Governance, Identity and access management	Governance and Ecosystem
Applicable - implemented	A.5.5	Contact with authorities	Organizational controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Identify, Protect, Respond, Recover	Governance	Defence, Resilience
Applicable - implemented	A.5.6	Contact with special interest groups	Organizational controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Protect, Respond, Recover	Governance	Defence
Applicable - implemented	A.5.7	Threat intelligence	Organizational controls	Preventive, Detective, Corrective	Confidentiality, Integrity, Availability	Identify, Detect, Respond	Threat and vulnerability management	Defence, Resilience
Applicable - implemented	A.5.8	Information security in project management	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Governance	Governance and Ecosystem, Protection
Applicable - implemented	A.5.9	Inventory of information and other associated assets	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Asset management	Governance and Ecosystem, Protection
Applicable - implemented	A.5.10	Acceptable use of information and other associated assets	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection	Governance and Ecosystem, Protection
Applicable - implemented	A.5.11	Return of assets	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management	Protection
Applicable - implemented	A.5.12	Classification of information	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Information protection	Protection, Defence
Applicable - implemented	A.5.13	Labelling of information	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Information protection	Protection, Defence
Applicable - implemented	A.5.14	Information transfer	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection	Protection
Applicable - implemented	A.5.15	Access control	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.5.16	Identity management	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.5.17	Authentication information	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.5.18	Access rights	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.5.19	Information security in supplier relationships	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Supplier relationships security	Governance and Ecosystem, Protection
Applicable - implemented	A.5.20	Addressing information security within supplier agreements	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Supplier relationships security	Governance and Ecosystem, Protection
Applicable - implemented	A.5.21	Managing information security in the ICT supply chain	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Supplier relationships security	Governance and Ecosystem, Protection
Applicable - implemented	A.5.22	Monitoring, review and change management of supplier services	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Supplier relationships security, Information security assurance	Governance and Ecosystem, Protection, Defence
Applicable - implemented	A.5.23	Information security for use of cloud services	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Protect	Supplier relationships security	Governance and Ecosystem, Protection
Applicable - implemented	A.5.24	Information security incident management planning and preparation	Organizational controls	Corrective	Confidentiality, Integrity, Availability	Respond, Recover	Governance, Information security event management	Defence
Applicable - implemented	A.5.25	Assessment and decision on information security events	Organizational controls	Detective	Confidentiality, Integrity, Availability	Detect, Respond	Information security event management	Defence
Applicable - implemented	A.5.26	Response to information security incidents	Organizational controls	Corrective	Confidentiality, Integrity, Availability	Respond, Recover	Information security event management	Defence
Applicable - implemented	A.5.27	Learning from information security incidents	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Information security event management	Defence
Applicable - implemented	A.5.28	Collection of evidence	Organizational controls	Corrective	Confidentiality, Integrity, Availability	Detect, Respond	Information security event management	Defence
Applicable - implemented	A.5.29	Information security during disruption	Organizational controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Protect, Respond	Continuity	Protection, Resilience
Applicable - implemented	A.5.30	ICT readiness for business continuity	Organizational controls	Corrective	Availability	Respond	Continuity	Resilience

esri UK & Ireland
THE SCIENCE OF WHERE

Applicability	Activity reference	Control / Activity	Objective / Deliverable	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
Applicable - implemented	A.5.31	Legal, statutory, regulatory and contractual requirements	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Legal and compliance	Governance and Ecosystem, Protection
Applicable - implemented	A.5.32	Intellectual property rights	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify	Legal and compliance	Governance and Ecosystem
Applicable - implemented	A.5.33	Protection of records	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Asset management, Information protection, Legal and compliance	Defence
Applicable - implemented	A.5.34	Privacy and protection of PII	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Information protection, Legal and compliance	Protection
Applicable - implemented	A.5.35	Independent review of information security	Organizational controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Identify, Protect	Information security assurance	Governance and Ecosystem
Applicable - implemented	A.5.36	Compliance with policies, rules and standards for information security	Organizational controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Legal and compliance, Information security assurance	Governance and Ecosystem
Applicable - implemented	A.5.37	Documented operating procedures	Organizational controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Protect, Recover	Asset management, Physical security, System and network security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Information security event management	Governance and Ecosystem, Protection, Defence
Applicable - implemented	A.6.1	Screening	People controls	Preventive	Confidentiality, Integrity, Availability	Protect	Human resource security	Governance and Ecosystem
Applicable - implemented	A.6.2	Terms and conditions of employment	People controls	Preventive	Confidentiality, Integrity, Availability	Protect	Human resource security	Governance and Ecosystem
Applicable - implemented	A.6.3	Information security awareness, education and training	People controls	Preventive	Confidentiality, Integrity, Availability	Protect	Human resource security	Governance and Ecosystem
Applicable - implemented	A.6.4	Disciplinary process	People controls	Preventive, Corrective	Confidentiality, Integrity, Availability	Protect, Respond	Human resource security	Governance and Ecosystem
Applicable - implemented	A.6.5	Responsibilities after termination or change of employment	People controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Human resource security	Governance and Ecosystem
Applicable - implemented	A.6.6	Confidentiality or non-disclosure agreements	People controls	Preventive	Confidentiality	Protect	Information protection, Human resource security, Supplier relationships security	Governance and Ecosystem
Applicable - implemented	A.6.7	Remote working	People controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection, Physical security, System and network security	Protection
Applicable - implemented	A.6.8	Information security event reporting	People controls	Detective	Confidentiality, Integrity, Availability	Detect	Information security event management	Defence
Applicable - implemented	A.7.1	Physical security perimeter	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Physical security	Protection
Applicable - implemented	A.7.2	Physical entry	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Physical security, Identity and access management	Protection
Applicable - implemented	A.7.3	Securing offices, rooms and facilities	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Physical security	Protection
Applicable - implemented	A.7.4	Physical security monitoring	Physical controls	Preventive, Detective	Confidentiality, Integrity, Availability	Protect, Detect	Physical security	Protection, Defence
Applicable - implemented	A.7.5	Protecting against physical and environmental threats	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Physical security	Protection
Applicable - implemented	A.7.6	Working in secure areas	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Physical security	Protection
Applicable - implemented	A.7.7	Clear desk and clear screen	Physical controls	Preventive	Confidentiality	Protect	Physical security	Protection
Applicable - implemented	A.7.8	Equipment siting and protection	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Physical security	Protection
Applicable - implemented	A.7.9	Security of assets off-premises	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Physical security	Protection
Applicable - implemented	A.7.10	Storage media	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Physical security	Protection
Applicable - implemented	A.7.11	Supporting utilities	Physical controls	Preventive, Detective	Integrity, Availability	Protect, Detect	Physical security	Protection
Applicable - implemented	A.7.12	Cabling security	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Physical security	Protection
Applicable - implemented	A.7.13	Equipment maintenance	Physical controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Physical security	Protection, Resilience

esri UK & Ireland
THE SCIENCE OF WHERE

Applicability	Activity reference	Control / Activity	Objective / Deliverable	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
Applicable - implemented	A.7.14	Secure disposal or re-use of equipment	Physical controls	Preventive	Confidentiality	Protect	Asset management, Physical security	Protection
Applicable - implemented	A.8.1	User endpoint devices	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Asset management, Information protection	Protection
Applicable - implemented	A.8.2	Privileged access rights	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.8.3	Information access restriction	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.8.4	Access to source code	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Application security, Secure configuration, Identity and access management	Protection
Applicable - implemented	A.8.5	Secure authentication	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Identity and access management	Protection
Applicable - implemented	A.8.6	Capacity management	Technological controls	Preventive, Detective	Integrity, Availability	Identify, Protect, Detect	Continuity	Governance and Ecosystem, Protection
Applicable - implemented	A.8.7	Protection against malware	Technological controls	Preventive, Detective, Corrective	Confidentiality, Integrity, Availability	Protect, Detect	Information protection, System and network security	Protection, Defence
Applicable - implemented	A.8.8	Management of technical vulnerabilities	Technological controls	Preventive	Confidentiality, Integrity, Availability	Identify, Protect	Threat and vulnerability management	Governance and Ecosystem, Protection, Defence
Applicable - implemented	A.8.9	Configuration management	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Secure configuration	Protection
Applicable - implemented	A.8.10	Information deletion	Technological controls	Preventive	Confidentiality	Protect	Information protection, Legal and compliance	Protection
Applicable - implemented	A.8.11	Data masking	Technological controls	Preventive	Confidentiality	Protect	Information protection	Protection
Applicable - implemented	A.8.12	Data leakage prevention	Technological controls	Preventive, Detective	Confidentiality	Protect, Detect	Information protection	Protection, Defence
Applicable - implemented	A.8.13	Information backup	Technological controls	Corrective	Integrity, Availability	Recover	Continuity	Protection
Applicable - implemented	A.8.14	Redundancy of information processing facilities	Technological controls	Preventive	Availability	Protect	Asset management, Continuity	Protection, Resilience
Applicable - implemented	A.8.15	Logging	Technological controls	Detective	Confidentiality, Integrity, Availability	Detect	Information security event management	Protection, Defence
Applicable - implemented	A.8.16	Monitoring activities	Technological controls	Detective, Corrective	Confidentiality, Integrity, Availability	Detect, Respond	Information security event management	Defence
Applicable - implemented	A.8.17	Clock synchronization	Technological controls	Detective	Integrity	Protect, Detect	Information security event management	Protection, Defence
Applicable - implemented	A.8.18	Use of privileged utility programs	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security, Secure configuration	Protection
Applicable - implemented	A.8.19	Installation of software on operational systems	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Application security, Secure configuration	Protection
Applicable - implemented	A.8.20	Networks security	Technological controls	Preventive, Detective	Confidentiality, Integrity, Availability	Protect, Detect	System and network security	Protection
Applicable - implemented	A.8.21	Security of network services	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security	Protection
Applicable - implemented	A.8.22	Segregation in networks	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security	Protection
Applicable - implemented	A.8.23	Web filtering	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security	Protection
Applicable - implemented	A.8.24	Use of cryptography	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Secure configuration	Protection
Applicable - implemented	A.8.25	Secure development life cycle	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection
Applicable - implemented	A.8.26	Application security requirements	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection, Defence
Applicable - implemented	A.8.27	Secure system architecture and engineering principles	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection
Applicable - implemented	A.8.28	Secure coding	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection
Applicable - implemented	A.8.29	Security testing in development and acceptance	Technological controls	Preventive	Confidentiality, Integrity, Availability	Identify	System and network security, Application security, Information security assurance	Protection
Applicable - implemented	A.8.30	Outsourced development	Technological controls	Preventive, Detective	Confidentiality, Integrity, Availability	Identify, Protect, Detect	System and network security, Application security, Supplier relationships security	Governance and Ecosystem, Protection
Applicable - implemented	A.8.31	Separation of development, test and production environments	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection
Applicable - implemented	A.8.32	Change management	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	System and network security, Application security	Protection
Applicable - implemented	A.8.33	Test information	Technological controls	Preventive	Confidentiality, Integrity	Protect	Information protection	Protection

Applicability	Activity reference	Control / Activity	Objective / Deliverable	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
Applicable - implemented	A.8.34	Protection of information systems during audit testing	Technological controls	Preventive	Confidentiality, Integrity, Availability	Protect	Information protection, System and network security	Governance and Ecosystem, Protection