  
Perera R.Y IT22552488

**Statement of Applicability (SoA) for ISO 27001:2022**

|  |  |  |  |
| --- | --- | --- | --- |
| Control Number | Control Description | Applicable (Yes/No/Partial) | Justification |
| A.5: Organizational Controls | | | |
| A.5.1 | Policies for information security | Yes | Information security policies are defined, approved, communicated, and reviewed at planned intervals. |
| A.5.2 | Information security roles and responsibilities | Yes | Information security roles are clearly defined and allocated. |
| A.5.3 | Segregation of duties | Yes | Conflicting duties are segregated to prevent fraud and misuse. |
| A.5.4 | Management responsibilities | Yes | Management ensures compliance with information security policies. |
| A.5.5 | Contact with authorities | Yes | Procedures are established for contacting relevant authorities. |
| A.5.6 | Contact with special interest groups | Yes | The organization maintains contact with security forums and associations. |
| A.5.7 | Threat intelligence | Yes | Threat intelligence is collected and analyzed to stay informed about new risks. |
| A.5.8 | Information security in project management | Yes | Information security is integrated into project management processes. |
| A.5.9 | Inventory of information and other associated assets | Yes | An asset inventory is developed and maintained, including asset owners. |
| A.5.10 | Acceptable use of information and other associated assets | Yes | Rules for acceptable use of assets are documented and enforced. |
| A.5.11 | Return of assets | Yes | Procedures are in place for returning assets upon termination or change. |
| A.5.12 | Classification of information | Yes | Information is classified based on confidentiality, integrity, and availability. |
| A.5.13 | Labelling of information | Yes | Procedures are in place for labelling information in accordance with classification. |
| A.5.14 | Information transfer | Yes | Information transfer rules and procedures are documented and enforced. |
| A.5.15 | Access control | Yes | Rules for physical and logical access control are established. |
| A.5.16 | Identity management | Yes | The full identity lifecycle is managed, including provisioning and de-provisioning. |
| A.5.17 | Authentication information | Yes | Authentication information is managed through secure processes. |
| A.5.18 | Access rights | Yes | Access rights are managed, reviewed, and modified as necessary. |
| A.5.19 | Information security in supplier relationships | Yes | Supplier security requirements are defined and implemented. |
| A.5.20 | Addressing information security within supplier agreements | Yes | Information security requirements are established in supplier agreements. |
| A.5.21 | Managing information security in the ICT supply chain | Yes | ICT supply chain security risks are managed through defined processes. |
| A.5.22 | Monitoring, review, and change management of supplier services | Yes | Supplier security practices are regularly monitored, reviewed, and updated. |
| A.5.23 | Information security for use of cloud services | Yes | Information security processes are in place for managing cloud services. |
| A.5.24 | Information security incident management planning and preparation | Yes | Plans and procedures are in place for managing security incidents. |
| A.5.25 | Assessment and decision on information security events | Yes | Information security events are assessed and categorized as incidents when appropriate. |
| A.5.26 | Response to information security incidents | Yes | Documented procedures are in place to respond to security incidents. |
| A.5.27 | Learning from information security incidents | Yes | Lessons learned from security incidents are used to improve controls. |
| A.5.28 | Collection of evidence | Yes | Procedures are in place for the collection of evidence in security incidents. |
| A.5.29 | Information security during disruption | Yes | Security controls are maintained during disruptions. |
| A.5.30 | ICT readiness for business continuity | Yes | ICT systems are tested and maintained for business continuity. |
| A.5.31 | Legal, statutory, regulatory, and contractual requirements | Yes | Legal, statutory, and regulatory requirements are identified and monitored. |
| A.5.32 | Intellectual property rights | Yes | Procedures are in place to protect intellectual property rights. |
| A.5.33 | Protection of records | Yes | Records are protected from loss, destruction, and unauthorized access. |
| A.5.34 | Privacy and protection of personally identifiable information (PII) | Yes | Procedures are in place to protect PII in line with applicable laws. |
| A.5.35 | Independent review of information security | Yes | Independent reviews of information security are conducted regularly. |
| A.5.36 | Compliance with policies, rules, and standards for information security | Yes | Compliance with information security policies is regularly reviewed. |
| A.5.37 | Documented operating procedures | Yes | Operating procedures are documented and made available to relevant personnel. |
| A.6: People Controls | | | |
| A.6.1 | Screening | Yes | Screening processes are in place, such as pre-employment background checks and ongoing checks for roles with access to sensitive information. |
| A.6.2 | Terms and conditions of employment | Yes | Standard employment contracts include specific information security and confidentiality clauses. |
| A.6.3 | Information security awareness, education, and training | Yes | Regular awareness, education, and training programs are provided, including role-based training and periodic updates. |
| A.6.4 | Disciplinary process | Yes | A formal disciplinary process is in place to handle information security violations. |
| A.6.5 | Responsibilities after termination or change of employment | Yes | Responsibilities are enforced and communicated to employees during exit interviews, and these are included in contracts. |
| A.6.6 | Confidentiality or non-disclosure agreements | Yes | NDAs and confidentiality clauses are included in all agreements with employees, contractors, and suppliers. |
| A.6.7 | Remote working | Yes | Security measures such as a home-working policy and technical controls are implemented for employees working remotely. |
| A.6.8 | Information security event reporting | Yes | A mechanism is in place for employees to report observed or suspected security events through appropriate channels. |
| A.7: Physical Controls | | | |
| A.7.1 | Physical security perimeters | Yes | Security perimeters are established to protect sensitive areas containing information and assets. |
| A.7.2 | Physical entry | Yes | Secure areas are protected by appropriate entry controls and access points. |
| A.7.3 | Securing offices, rooms, and facilities | Yes | Physical security controls are implemented for offices and facilities to prevent unauthorized access. |
| A.7.4 | Physical security monitoring | Yes | Continuous monitoring is performed for unauthorized physical access through CCTV and other systems. |
| A.7.5 | Protecting against physical and environmental threats | Yes | Measures are in place to protect against environmental threats, such as natural disasters and other risks. |
| A.7.6 | Working in secure areas | Yes | Security measures are implemented to manage risks associated with working in secure areas. |
| A.7.7 | Clear desk and clear screen | Yes | Clear desk policies and screen lock policies are enforced to protect sensitive information. |
| A.7.8 | Equipment siting and protection | Yes | Equipment is properly sited and protected to minimize the risk of unauthorized access. |
| A.7.9 | Security of assets off-premises | Yes | Policies are in place to ensure that assets taken off premises are protected. |
| A.7.10 | Storage media | Yes | Storage media is managed throughout its lifecycle in accordance with classification and handling requirements. |
| A.7.11 | Supporting utilities | Yes | Facilities are protected from power failures and other disruptions caused by supporting utilities. |
| A.7.12 | Cabling security | Yes | Cables carrying power, data, or supporting information services are secured against interception and damage. |
| A.7.13 | Equipment maintenance | Yes | Equipment is regularly maintained to ensure availability, integrity, and confidentiality of information. |
| A.7.14 | Secure disposal or re-use of equipment | Yes | Procedures are in place to ensure that sensitive data is removed or securely overwritten before equipment disposal or re-use. |
| A.8: Technological Controls | | | |
| A.8.1 | User endpoint devices | Yes | Information stored on, processed by, or accessible via user endpoint devices is protected through encryption and remote disablement. |
| A.8.2 | Privileged access rights | Yes | The allocation and use of privileged access rights are restricted and managed through role-based access control. |
| A.8.3 | Information access restriction | Yes | Access to information and associated assets is restricted based on established access control policies. |
| A.8.4 | Access to source code | Yes | Access to source code, development tools, and software libraries is appropriately managed and restricted to authorized personnel only. |
| A.8.5 | Secure authentication | Yes | Secure authentication technologies and procedures are implemented based on access control policies. |
| A.8.6 | Capacity management | Yes | The use of resources is monitored and adjusted in line with current and expected capacity requirements. |
| A.8.7 | Protection against malware | Yes | Protection against malware is implemented with appropriate user awareness training and technical controls. |
| A.8.8 | Management of technical vulnerabilities | Yes | Technical vulnerabilities are evaluated, and appropriate measures are taken, including patching and security updates. |
| A.8.9 | Configuration management | Yes | Security configurations of hardware, software, services, and networks are established, documented, and monitored. |
| A.8.10 | Information deletion | Yes | Information stored in systems or storage media is deleted when no longer required according to retention policies. |
| A.8.11 | Data masking | Yes | Data masking techniques are applied to safeguard personally identifiable information. |
| A.8.12 | Data leakage prevention | Yes | Data leakage prevention measures are implemented to protect sensitive information across systems and networks. |
| A.8.13 | Information backup | Yes | Backup copies of information and systems are maintained and regularly tested according to policies. |
| A.8.14 | Redundancy of information processing facilities | Yes | Redundancy measures are implemented to ensure availability requirements are met for information processing facilities. |
| A.8.15 | Logging | Yes | Logs of activities, exceptions, and faults are produced, stored, protected, and analyzed for security purposes. |
| A.8.16 | Monitoring activities | Yes | Systems and networks are monitored for anomalous behavior to detect potential security incidents. |
| A.8.17 | Clock synchronization | Yes | Clocks of information processing systems are synchronized to approved time sources. |
| A.8.18 | Use of privileged utility programs | Yes | The use of utility programs capable of overriding system controls is restricted and tightly controlled. |
| A.8.19 | Installation of software on operational systems | Yes | Procedures are implemented to manage software installations securely on operational systems. |
| A.8.20 | Networks security | Yes | Network devices are secured, managed, and controlled to protect information systems. |
| A.8.21 | Security of network services | Yes | Security mechanisms and service requirements for network services are identified and monitored. |
| A.8.22 | Segregation of networks | Yes | Segregation of groups of information services and systems is enforced to manage risks. |
| A.8.23 | Web filtering | Yes | Access to external websites is managed to reduce exposure to malicious content. |
| A.8.24 | Use of cryptography | Yes | Effective use of cryptography, including key management, is defined and implemented. |
| A.8.25 | Secure development life cycle | Yes | Rules for secure software and system development are established and applied. |
| A.8.26 | Application security requirements | Yes | Information security requirements are identified and approved during application development or acquisition. |
| A.8.27 | Secure system architecture and engineering principles | Yes | Secure system engineering principles are documented and applied during development activities. |
| A.8.28 | Secure coding | Yes | Secure coding practices are enforced during software development to mitigate vulnerabilities. |
| A.8.29 | Security testing in development and acceptance | Yes | Security testing processes are defined and implemented in the development life cycle. |
| A.8.30 | Outsourced development | Not Applicable | IFS do not use outsourced development resources for its products. |
| A.8.31 | Separation of development, test, and production environments | Yes | Development, testing, and production environments are separated to manage risks. |
| A.8.32 | Change management | Yes | Changes to information processing facilities and systems are subject to defined change management procedures. |
| A.8.33 | Test information | Yes | Test data is selected, protected, and managed appropriately. |
| A.8.34 | Protection of information systems during audit testing | Yes | Audit tests and assurance activities are planned and agreed upon to ensure security during assessments. |