



Adeption SOA

Version Number	Date	Type	Description	Prepared By	Reviewed By	Approved By
V1.0	9/7/2024	Final	Initial Publication Version	Milind Panchanadikar (database developer)	Tim Winstone(COO)	Amol Deshpande(CISO)
V1.0	7/11/2024	Final	Board approved Version	Milind Panchanadikar (database developer)	All heads of Departments	Board of Directors
V1.0	8/8/2025	Final	Updated Chairperson	Milind Panchanadikar (database developer)	All heads of Departments	Board of Directors
V1.0	6/11/2025	Final	Updated Board Approval	Milind Panchanadikar (database developer)	All heads of Departments	Board of Directors
V1.1	27/07/2026	Final	Updated latest links	Nikita Jain (Global HR and Operations Manager)	Tim Winstone(COO) and Amol Deshpande (CTO)	Raksha Nirwan (CISO)

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
1	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	PO001 - Information Security Policy.pdf	Yes	To achieve company objective of providing customers leadership coaching using B3 methodology with information security, confidentiality and availability of the information resources at all times.
2	5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	ISMS Governance Team-Skill Matrix	Yes	Identifying responsibility and establishing accountability in implementing the IS policies is best achieved by laying down roles and responsibilities for ISMS in the organization hierarchy.
3	5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	PR012-Segregation of Duties (SoD) Procedure.pdf	Yes	Effective management of internal controls requires that no single person is in charge of internal control of IT processes and for improved effectiveness of the controls segregation of duty is essential.
4	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.	Adeption_Roles_and_InfoSec_Responsibilities - All Employees.xlsx 2026.xlsx	Yes	Accountability will be established from the employees when formal contracts are executed
5	5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Emergency Contact Number	Yes	Appropriate contacts with the relevant authorities are handy in case of security incidents and facility related issues.
6	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.	Contact list of Special Interest Group	Yes	Company would like to address its international business issues more effectively when it is part of support group of companies, trade or association
7	5.7	Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	PO039 - Threat Intelligence Policy.pdf	Yes	Threat intelligence is essential for proactively identifying, assessing, and mitigating evolving cyber threats, enabling organizations to enhance security, manage risks, ensure compliance, and minimize financial and reputational damage.
8	5.8	Information security in project management	Information security should be integrated into project management.	PO036 - System Planning and Acceptance Policy.pdf	Yes	Timely execution of the development projects in Adeption application with optimum resources and security of data, privacy and its software is prime important for the project management.
9	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	PO003 - Asset Management Policy.pdf PO023 - Information Security Risk Management Framework Policy.pdf	Yes	Information assets are effectively managed when inventory and the status is known which provides valuable information for adequacy of the processing facilities. Ownership of the assets would enable the management to fix accountability for its upkeep,maintenance. damage or loss
10	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.	PO019 - Acceptable Use Policy.pdf	Yes	Unrestricted and unacceptable usage need to be communicated to all the stakeholders in order to ensure right attitude and manner of protecting the informationasset
11	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.	PO003 - Asset Management Policy.pdf PO016 - Human Resources Security Policy.pdf PR020-Offboarding Procedure.pdf	Yes	To achieve the objective of the exit policy for the employees appropriate controls like return of assets and clearance of dues is necessary

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
12	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.	PO027 - Information Classification and Handling Policy.pdf	Yes	Company has to deal with huge amount of information flowing in and out of the organization, the appropriate protection can be offered only when the information is classified such as confidential, internal, public etc.
13	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.	PO027 - Information Classification and Handling Policy.pdf	Yes	Company has to deal with huge amount of information flowing in and out of the organization, the appropriate protection can be offered only when the information classified is appropriately labelled.
14	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.	PO007 - Communication and Network Security Policy.pdf PO033 - Email Security Policy.pdf PO019 - Acceptable Use Policy.pdf	Yes	Commitments to customers require secured transmission of information through all types of communication facilities
15	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.	PO002 - Access Control Policy.pdf PO028 - Identity Management Policy.pdf PO043 - Password Policy.pdf https://adeption-isms.azurewebsites.net/access-management/subscription-matrix	Yes	Company's policy of providing access on need to do basis is best achieved through access control policy
16	5.16	Identity management	The full life cycle of identities should be managed.	PO028 - Identity Management Policy.pdf PO002 - Access Control Policy.pdf	Yes	Identity management is crucial for ensuring secure access control, preventing unauthorized access, reducing insider threats, maintaining compliance, and managing user identities efficiently throughout their lifecycle from creation to deactivation.
17	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.	PO002 - Access Control Policy.pdf PO028 - Identity Management Policy.pdf PO043 - Password Policy.pdf	Yes	Application level admin access and super user access when controlled with procedure will ensure availability of secret credentials to the top management
18	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	PO002 - Access Control Policy.pdf PO028 - Identity Management Policy.pdf	Yes	Access should be provided only on need to do basis and should be periodically reviewed. RBAC principle should be followed while providing access.
19	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.	PO010 - Vendor Security Policy.pdf PO020 - Third-Party Access Policy.pdf Access Control Matrix for vendor List- Vendor List Agreement for 2026 Audit Vendor NDA	Yes	Vendor management and security considerations provide smooth and easy monitoring of vendor SLA performance.
20	5.20	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	PO010 - Vendor Security Policy.pdf	Yes	Vendor management and security considerations provide smooth and easy monitoring of vendor SLA performance.
21	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.	PO010 - Vendor Security Policy.pdf	Yes	Vendor management and security considerations provide smooth and easy monitoring of vendor SLA performance and prevent disruptions
22	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.	PO010 - Vendor Security Policy.pdf	Yes	Monitoring and review of supplier services help to improve customer services and security.
23	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.	PO022 - Cloud Security Policy.pdf	Yes	Establishing processes for cloud service usage is essential to ensure data security, compliance, risk management, and seamless transitions while preventing unauthorized access and data breaches.

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
24	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.	PO013 - Incident Management Policy.pdf	Yes	Planning and preparing for information security incidents is crucial to ensure a swift, coordinated response that minimizes damage, reduces downtime, maintains compliance, and enhances overall cybersecurity resilience.
25	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.	PO013 - Incident Management Policy.pdf	Yes	Incident Management Procedure when implemented will prevent incident growing into crisis.
26	5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	PO013 - Incident Management Policy.pdf	Yes	Incident Management Procedure when implemented will prevent incident growing into crisis.
27	5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	PO013 - Incident Management Policy.pdf	Yes	Incident management procedure providing learning from security incidents would help to recurrence of the similar incidents.
28	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.	PO013 - Incident Management Policy.pdf	Yes	Incident Management Procedure when implemented will prevent incident growing into crisis.
29	5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	PO014 - Business Continuity and Disaster Recovery Policy.pdf	Yes	Maintaining information security during disruptions is essential to protect sensitive data, ensure business continuity, prevent cyber threats, and comply with regulatory requirements even in crisis situations.
30	5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	PO014 - Business Continuity and Disaster Recovery Policy.pdf	Yes	Testing of DR and BCP will provide preparedness and resilience in the event of disruption of the business.
31	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	PO026 - Compliance, Legal and Privacy Policy.pdf	Yes	Legal compliance requirement
32	5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	PO037 - Intellectual Property (IP) Policy.pdf	Yes	Legal compliance would be ensured when the procedure for IP management is implemented and records maintained
33	5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	PO030 - Document Control and Record Retention Policy.pdf	Yes	Protection and retention of the data in all its forms is necessary from legal compliance and forensic point of view.
34	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.	PO018 - Data Privacy and Protection Policy.pdf	Yes	legal requirement and Business Requirement
35	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.	PO038 - Internal Audit Policy and Procedure.pdf	Yes	Independent review of information security is a tool for providing improvements in the control activities.
36	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.	PO001 - Information Security Policy.pdf	Yes	Review of the policies would help to keep the updated security framework and would adapt to changes in the risk profile of the business of the company
37	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them	PO006 - Operations Security Policy.pdf	Yes	Documented procedures would provide precise direction to the employees and management a clear direction to implement and monitor the information security

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
38	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.	PO016 - Human Resources Security Policy.pdf	Yes	One of the ways of ensuring that the employees are onboarded with acceptable level of experience, integrity and background is to have an independent back ground screening of the new employees.
39	6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security	PO016 - Human Resources Security Policy.pdf	Yes	Accountability will be established from the employees when formal contracts are executed
40	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.	PO035 - Training and Awareness Policy.pdf	Yes	Awareness of Information security enables the company management to achieve its objective with higher level of maturity
41	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.	PO025 - Disciplinary Action Policy.pdf	Yes	To enforce information security implementation a disciplinary actions is imperative.
42	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.	PO016 - Human Resources Security Policy.pdf	Yes	Contractual and Legal requirements
43	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.	PO024 - Data Confidentiality Policy.pdf	Yes	Contractual and Legal requirements
44	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.	PO017 - Mobile Device and Remote Working Policy.pdf	Yes	Remote access to company's cloud resources and networks has necessitated that the remote working be strictly controlled.
45	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.	PO013 - Incident Management Policy.pdf	Yes	Incident Management Procedure when implemented will prevent incident growing into crisis.
46	7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Physical access control like guard and surveillance provide prevention of unauthorised persons entering the facility containing sensitive information or processing facility
47	7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Physical access control like guard and surveillance provide prevention of unauthorised persons entering the facility containing sensitive information or processing facility
48	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Physical access control like guard and surveillance provide prevention of unauthorised persons entering the facility containing sensitive information or processing facility
49	7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access	PO005 - Physical and Environmental Security Policy.pdf	Yes	Physical access control like guard and surveillance provide prevention of unauthorised persons entering the facility containing sensitive information or processing facility
50	7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Customer SLA requires for uninterrupted support service drives the DR and BCP implementation.

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
51	7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented	PO005 - Physical and Environmental Security Policy.pdf	Yes	Secured facilities provides protection to the people, processes and equipments
52	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.	PO040 - Clean Desk Policy.pdf	Yes	Will help ensure that all sensitive/confidential materials are removed from workspaces and locked away when the items are not in use or an employee leaves their workstation. The policy will help reduce the risk of security breaches within the workplace.
53	7.8	Equipment siting and protection	Equipment should be sited securely and protected.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Customer SLA requires for uninterrupted support service drives the DR and BCP implementation.
54	7.9	Security of assets off-premises	Off-site assets should be protected	PO017 - Mobile Device and Remote Working Policy.pdf	Yes	No equipment of the compny is placed off the premises requiring information security
55	7.10	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.	PO003 - Asset Management Policy.pdf	Yes	Appropriate procedure for handling of information according to its nature and classification is prime factor in information handling
56	7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Customer SLA requires for uninterrupted support service drives the DR and BCP implementation.
57	7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	PO005 - Physical and Environmental Security Policy.pdf	Yes	Exclusive data cables would protect the intrusion of company's data transmission
58	7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	PO006 - Operations Security Policy.pdf	Yes	Preventive maintenance ensures continued availability and operations and will comply the SLA
59	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.	PO003 - Asset Management Policy.pdf	Yes	To make sure no proprietary or confidential data falls into unauthorised persons.
60	8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected	PO017 - Mobile Device and Remote Working Policy.pdf	Yes	Protecting user endpoint devices is essential to prevent data breaches, mitigate security risks, ensure compliance, and safeguard sensitive information from unauthorized access or cyber threats.
61	8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	PO002 - Access Control Policy.pdf	Yes	Privilege users are high risk if not managed as per the security policy.
62	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.	PO002 - Access Control Policy.pdf	Yes	Commitment to customers SLA is achieved when access control is established
63	8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	PO011 - Secure Development and Coding Policy.pdf	Yes	To prevent other than project team development members to tamper with the source code and other utilities
64	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.	PO043 - Password Policy.pdf	Yes	To prevent to damage and application from unauthorised access secured logon procedure is adopted
65	8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	PO006 - Operations Security Policy.pdf	Yes	To prevent unforeseen instance of capacity of the servers being inadequate for continued operations.
66	8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness	PO006 - Operations Security Policy.pdf	Yes	To prevent disruption due to malware and damage to the data
67	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.	PO032 - Technical Vulnerability Management Policy.pdf	Yes	Pro-active technical vulnerabilities would enable the process owners to strengthen security against cyber attacks

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
68	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	PO006 - Operations Security Policy.pdf	Yes	Effective configuration management is essential to ensure system integrity, reduce vulnerabilities, prevent misconfigurations, enhance security, and maintain compliance by continuously monitoring and managing hardware, software, and network settings.
69	8.10	Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	PO003 - Asset Management Policy.pdf	Yes	Proper information deletion is crucial to prevent unauthorized access, reduce security risks, ensure compliance with data protection regulations, and minimize unnecessary data retention.
70	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.	PO044 - Data Masking Policy.docx.pdf	Yes	Data masking is not required due to the low sensitivity of stored PII, but may be applied in specific scenarios such as test environments, logging, or analytics datasets.
71	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.	PO029 - Data Leakage Prevention (DLP) Policy.pdf	Yes	Data leakage prevention is crucial to safeguard sensitive information, prevent unauthorized disclosures, mitigate insider threats, ensure regulatory compliance, and protect an organization's reputation and assets.
72	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.	PO008 - Backup and Recovery Policy.pdf	Yes	to ensure that the data for the projects, customers and authorities is available and recoverable in case of security incident.
73	8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements	PO014 - Business Continuity and Disaster Recovery Policy.pdf	Yes	Business continuity planning is essential for uninterrupted operations and early resumption
74	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	PO009 - Logging and Monitoring Policy.pdf	Yes	Logs monitoring would help detect any unknown and unauthorised transactio
75	8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	PO009 - Logging and Monitoring Policy.pdf	Yes	Monitoring and retaining logs would provide traceability
76	8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	PO034 - Clock Synchronization Policy.pdf	Yes	Facilitates investigation and forensic when clocks across the system servers are synchronized
77	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.	PO006 - Operations Security Policy.pdf	Yes	By nature of the business of the company certain application support function need to be overridden
78	8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	PO006 - Operations Security Policy.pdf	Yes	At the request of the customer in case any tool or software to be integrated with existing business system. we carryout the task with due approval.
79	8.20	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	PO007 - Communication and Network Security Policy.pdf	Yes	In house security mechanisms provide continuous monitoring and detect unauthorised network traffic
80	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	PO007 - Communication and Network Security Policy.pdf	Yes	In house security mechanisms provide continuous monitoring and detect unauthorised network traffic
81	8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.	PO007 - Communication and Network Security Policy.pdf	Yes	To strengthen data protection and prevent unauthorised access to critical servers
82	8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	PO007 - Communication and Network Security Policy.pdf	Yes	Web filtering is essential to prevent access to malicious websites, reduce cybersecurity risks, protect sensitive data, and ensure compliance with security policies.

Sr. No.	ISO 27001-2022 Controls	Control	Description	Document Reference	Applicability	Justification
83	8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	PO004 - Cryptographic Systems Policy.pdf	Yes	Customer demands that the transmission from app server to their systems to be confidential hence encryption is required
84	8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	PO011 - Secure Development and Coding Policy.pdf	Yes	Secured development standards embed security features in source codes.
85	8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	PO011 - Secure Development and Coding Policy.pdf	Yes	Defining application security requirements is essential to prevent vulnerabilities, protect sensitive data, ensure compliance, and maintain the integrity of software throughout its development and acquisition.
86	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.	PO011 - Secure Development and Coding Policy.pdf	Yes	Applying secure system architecture and engineering principles is crucial to build resilient systems, mitigate security risks, protect sensitive data, and ensure compliance throughout the system development lifecycle.
87	8.28	Secure coding	Secure coding principles should be applied to software development.	PO011 - Secure Development and Coding Policy.pdf	Yes	Applying secure coding principles is essential to prevent vulnerabilities, mitigate security risks, protect sensitive data, and ensure the reliability and compliance of software applications.
88	8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	PO011 - Secure Development and Coding Policy.pdf	Yes	Testing of security functionality would minimize the adverse impact in the output of the development.
89	8.30	Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	N/A	No	Adeption has in-house development team and does not outsource any system development
90	8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	PO011 - Secure Development and Coding Policy.pdf	Yes	Adeption has in-house development team and does not outsource any system development
91	8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures	PO012 - Change Management Policy.pdf	Yes	To provide traceability and accountability for every change to the company's system and infrastructure
92	8.33	Test information	Test information should be appropriately selected, protected and managed.	PO011 - Secure Development and Coding Policy.pdf	Yes	Secured test data helps to adhere to good practices
93	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.	PO038 - Internal Audit Policy and Procedure.pdf	Yes	Protecting information systems during audit testing is essential to prevent disruptions, maintain data integrity, ensure compliance, and mitigate security risks while conducting assessments.