Name of the Organization	AudiTree	
Address	35/2588A3, Pearl building Ponekkara Road Meenchira AIMS P.O, Edappally	
Additional Sites	NA	
No. of Employees	17	
No. of Shift	1	
Contact Person	Syeda Ghazala Nishath	
Designation	CISO	
E mail id	**ghazala.nishath@auditree.com**	
Telephone/Fax	+91 8296054512	
Business Activities / Processes	At AudiTree, we redefine auditing by focusing not just on compliance but on delivering strategic insights powered by AudiTree audit expertise that empower businesses. Our services are meticulously designed to enhance accuracy, minimize risks, and streamline financial operations. Whether through offshoring audit support or comprehensive financial solutions, our mission is to help companies drive efficiency, reduce overhead costs, and unlock growth potential.	
Scope	"The Information Security Management System (ISMS) of AudiTree covers the processes, information, and information systems supporting the delivery of all types of audit services (including external and internal audits provided through the offshoring model), finance transformation, and accounting support for client-developed ERP software - delivered from AudiTree employees' remote working locations	
Technical Area	Audit	
Audit Team	Lead Auditor: Dennis Anand.J Technical Expert: N/A	No of Man-days: 01
Starting date of Audit	22-01-2026	
End date of Audit	22-01-2026	
Brief about the organization	In today's fast-paced business environment, even the smallest details can have significant consequences. At AudiTree, our internal audit services are built around meticulous accuracy and strategic analysis, ensuring your financial statements are not only accurate but flawless.	

	Our comprehensive auditing process, from initial planning to the final report, is designed to be seamless and thorough. We collaborate closely with your team, scrutinizing every financial detail and proactively identifying potential issues. With a focus that extends beyond compliance, we provide actionable insights to strengthen your business. AudiTree enables you to stay focused on what matters most—driving growth.
Purpose of Audit	To verify the implementation of the Information Security Management System as per the ISO 27001:2022 Standard Requirement, verification of records for the conformity of the implementation.

CHANGE DETAIL:

Are quoted man-days adequate?	YES
Any change in employee detail?	NO
Any Change in Scope?	NO

Date of Audit: 22-01-2026

SUMMARY OF AUDIT

AREA OF IMPROVEMENTS / RECOMMENDATIONS	
For **AudiTree** this is the certification audit against the ISO/IEC 27001:2022 standard and with that regard the intent of the organization was the focus of the audit along with demonstrating compliance to the ISO 27001:2022 standard. **AudiTree's** scope and the respective ISMS controls are implemented accordingly, the ISMS forum headed by **Syeda Ghazala Nishath, CISO**– is accountable for **AudiTree** towards the ISMS standard. The ISMS is mapped to the ISO/IEC 27001:2022 standard, along with updates to respective changes in controls, policies and procedures. The Internal audits are planned and conducted regularly; the ISMS objectives and continual improvement initiatives are defined and tracked as per the schedule. Overall, the security posture of **AudiTree** fulfils the requirements of the ISO/IEC 27001:2022 with 0 Nonconformities identified during this certification audit.	
1.	Nil
2.	Nil
Non-Conformities Raised **__0__**Minor/Major Non-conformance identified in the audit, details of Non-Conformance in F50 *Please respond by using your own corrective action form and include the root cause analysis with systemic corrective action. Failure to include root cause analysis with systemic corrective action will result in your responses being rejected by Lead Auditor.*	
Team Leader Declaration (Tick or cross Each Column as per applicability)	
✓	Auditing is based on a sampling process of the available information
N/A	Audit is combined, joint or integrated;
N/A	The effectiveness of corrective actions taken regarding previously identified nonconformities have verified outcomes, are effective and complying.
✓	The internal audit and management review process are effective and complying with the requirements.
✓	The scope of certification is appropriate.
✓	The capability of the management system to meet applicable requirements and expected
✓	The audit objectives have been fulfilled and achieved.

Recommendation:

✓	**The Management system complies with the requirements of the reference standard:** Congratulations, based on the above summary, Lead Auditor is pleased to put forward a recommendation for Issuance of Certificate. The organization can use the Intercert Mark

	The quality system complies with the requirements of the reference standard with exception of minor NC: Congratulations, Team Leader is pleased to put forward a recommendation for Issuance of the certificate of Organization upon off-site verification of closure of all minor NC within 60 days from the date of Stage 2 audit. Responses to the non-conformances should be submitted to Intercert and must include supporting evidence of closure to allow for off-site verification. In responding to the non-conformances, the organization should consider the root cause of the non-conformance and the potential for related issues in other parts of system. If all non-conformances are not closed within 60 days, a full reassessment may be required.
	Evidence of major non-conformities: Organization is not recommended for Issuance of Certificate and currently. Follow-up audit will be scheduled to allow for on-site verification and closure of all issues within 60 days from the date of Stage 2. Once all non-conformances are closed, the recommendation for Issuance of certification may recommended. If all non-conformances are not closed within 60 days, a full reassessment may be required.
	Not Recommended: Organization is not recommended for Issuance of certificate at this time. Full Stage 2 audit is required as the organisation has not implemented the system and process at pace.
	Proposed Audit Date for 1st Surveillance Audit on or before 22-01-2027

Sign Off: (Date) 10-02-2026	
Intercert Audit Report Submission	Client Acceptance for Report
Name of Audit Team Leader: Dennis Anand.J 	Name: Designation:

Detailed Audit Report – ISO/IEC 27001:2022

VERIFICATION OF DOCUMENTED INFORMATION & RECORDS AS PER STD REQUIREMENT (C- Conformity, NC-Non-Conformity, O-Observation)		
ISO 27001-2022 ISMS Requirements	**C/NC/O**	**Comments**
4 - Context of the organisation -		
4.1 - **Understanding the organisation and its context** - The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system	**C**	Yes, the organisation has determined external and internal issues relevant to its purpose to achieve the ISMS. Verified ISMS Manual Version 1.0 Dated 18 August 2025.
4.2 - **Understanding the needs and expectations of interested parties** - The organisation shall determine: a) interested parties that are relevant to the information security management system - - b) the relevant requirements of these interested parties - - c) which of these requirements will be addressed through the information security management system.	**C**	Yes, the organisation has determined that all interested parties, and their requirements have been addressed by the ISMS. Verified ISMS Manual Version 1.0 Dated 18 August 2025.
4.3 **- Determining the scope of the information security management system** - The organisation shall determine the boundaries and applicability of the information security management system to establish its scope. - - When determining this scope, the organisation shall consider: a) the external and internal issues referred to in 4.1 - - b) the requirements referred to in 4.2	**C**	Yes, ISMS policy is documented and has considered external and internal issues. Verified ISMS Manual Version 1.0 Dated 18 August 2025.

- - c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations.		
4.4 - **Information security management system** - The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.	**C**	Yes, ISMS is established and documented. Verified ISMS Manual Version 1.0 Dated 18 August 2025. Verified SOA version V 1.0 dated 10-09-2025
5 - Leadership -		
5.1 - **Leadership and commitment** - Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organisation - - b) ensuring the integration of the information security management system requirements into the organisation's processes; - - c) ensuring that the resources needed for the information security management system are available; - - d) communicating the importance of effective information security management and of conforming to the information security management system requirements; - - e) ensuring that the information security management system achieves its intended outcome(s);	**C**	Yes, The Information Security team ensures the organisation's compliance towards the ISMS. Yes, Syeda Ghazala Nishath, CISO, is accountable for ISMS compliance and ensures the organisation's compliance towards the ISMS.

- - f) directing and supporting persons to contribute to the effectiveness of the information security management system; - - g) promoting continual improvement; and - - h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.		
5.2 - **Policy** - Top management shall establish an information security policy that: a) is appropriate to the purpose of the organisation; - - b) includes information security objectives or provides the framework for setting information security objectives; - - c) includes a commitment to satisfy applicable requirements related to information security; - - d) includes a commitment to continual improvement of the information security management system. - - The information security policy shall: e) be available as documented information; - - f) be communicated within the organisation; - - g) be available to interested parties, as appropriate.	**C**	ISMS policy is defined, reviewed and communicated to all the stakeholders & interested parties. Verified ISMS Manual Version 1.0 Dated 18 August 2025.
5.3 - **Organisational roles, responsibilities and authorities** - Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. Top management shall assign the responsibility and authority for: a) ensuring that the information security	**C**	The roles and responsibilities are mentioned in the information security roles and responsibilities document. Verified Information Security Roles and Responsibilities document.

management system conforms to the requirements of this document - - b) reporting on the performance of the information security management system to top management.		
6 - Planning -		
6.1 - Actions to address risks and opportunities -		
6.1.1 - General - When planning for the information security management system, the organisation shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); - - b) prevent, or reduce, undesired effects; - - c) achieve continual improvement. - - The organisation shall plan: d) actions to address these risks and opportunities; and - - e) how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	**C**	The risk management is detailed, all risks are identified, categorized by rating, assets are tagged to the respective risks and mitigation plans are defined, tested and reviewed annually. Verified Risk Management Framework. Verified Risk Register Version 1.0 Dated 18 August 2025
6.1.2 - Information security risk assessment - The organisation shall define and apply an information security risk assessment process that: - - a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and	**C**	A detailed and comprehensive risk assessment has been implemented and is reviewed annually. Verified Risk Management Framework.

2) criteria for performing information security risk assessments; - - b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; - - c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners - - d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2c) 1) were to materialise; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; - - e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment.		Verified Risk Register Version 1.0 Dated 18 August 2025

6.1.3 - Information security risk treatment - The organisation shall define and apply an information security risk treatment process to: - - a) select appropriate information security risk treatment options, taking account of the risk assessment results; - - b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; - - c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; - - d) produce a Statement of Applicability that contains - the necessary controls (see 6.1.3 b) and c)); - justification for their inclusion; - whether the necessary controls are implemented or not; and - the justification for excluding any of the Annex A controls. - - e) formulate an information security risk treatment plan; and - - f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. - - The organization shall retain documented information about the information security risk treatment process.	**C**	Yes, The IS risk treatment and mitigation in place and determines all the controls necessary to implement them. Verified Risk Management Framework. Verified Risk Register Version 1.0 Dated 18 August 2025
6.2 - **Information security objectives and planning to achieve them -**		

6.2 - General - The organisation shall establish information security objectives at relevant functions and levels. - - The information security objectives shall: a) be consistent with the information security policy - - b) be measurable (if practicable); - - c) take into account applicable information security requirements, and risk assessment and risk treatment results; - - d) be monitored - - e) be communicated - - f) be updated as appropriate - - g) be available as documented information The organization shall retain documented information on the information security objectives. - - When planning how to achieve its information security objectives, the organisation shall determine; h) what will be done; - - i) what resources will be required; - - j) who will be responsible; - - k) when it will be completed; and - - l) how the results will be evaluated.	**C**	Metric based objectives implemented and these are reviewed and analysed, and results discussed in the MRM. The latest Management Review Meeting was conducted on January 19, 2026
6.3 - When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner. -	**C**	Yes, the changes to ISMS are carried out in a planned manner.
7 - Support -		

7.1 - Resources - The organisation shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system. - - The organisation shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance. - - b) ensure that these persons are competent on the basis of appropriate education, training, or experience; - - c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and - - d) retain appropriate documented information as evidence of competence.	**C**	Yes, the resources are defined and managed suitably.
7.2 Competence Has the organization determined the necessary competence and ensure it, take actions to acquire, retain documentation? Documented Information. Evidence of competence.	**C**	Yes, organization tracks competency of all its resources
7.3 - Awareness - Persons doing work under the organisation's control shall be aware of: a) the information security policy; - - b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and	**C**	All employees are motivated to complete ISMS awareness every year. All New joiners are mandated to complete awareness training within a month of joining. Lastly ISMS awareness is provided on need basis to the respective stakeholder / interested parties

- - c) the implications of not conforming with the information security management system requirements.		
7.4 - Communication - The organisation shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) how to communicate	**C**	Only E-mails considered authorized form of communication channel with defined ways to communicate.
7.5.1 - **Documented information** General - The organisation's information security management system shall include: a) documented information required by this document; and b) documented information determined by the organisation as being necessary for the effectiveness of the information security management system. 7.5.2 - **Creating and updating** - When creating and updating documented information the organisation shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number) b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy. 7.5.3 - **Control of documented information** - Documented information required by the information security management system and by this document shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and	**C**	A detailed roles and responsibilities document covers the responsibilities for documentation creation to approval and distribution. Every document has document controls in place.

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organisation shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.		
8 **- Operation -**		
8.1 - **Operational planning and control** - The organisation shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6.2, by: - establishing criteria for the processes; - implementing control of the processes in accordance with the criteria. - - Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. - - The organisation shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. - - The organisation shall ensure that and externally provided processes, products or services that are	**C**	Yes, Operational planning is managed well by defining processes, performance metrics, objectives, implemented a change management.

relevant to the information security management system are controlled.		
8.2 - **Information security risk assessment** - The organisation shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). - - The organisation shall retain documented information of the results of the information security risk assessments.	**C**	Yes, Risk register exists and is verified, the same is reviewed at least annually. Verified Risk Register Version 1.0 Dated 18 August 2025 Verified Risk Management Framework.
8.3 - **Information security risk treatment** - The organisation shall implement the information security risk treatment plan. The organisation shall retain documented information of the results of the information security risk treatment. - - The organisation shall implement the information security risk treatment plan. The organisation shall retain documented information of the results of the information security risk treatment.	**C**	Yes, the risk register also captures the mitigation plans, some risks have multiple layers of mitigation based on the severity of the risk. Verified Risk Management Framework. Verified Risk Register Version 1.0 Dated 18 August 2025
9 - Performance evaluation -		
9.1 - Monitoring, measurement, analysis and evaluation - The organisation shall determine: a) what needs to be monitored and measured, including information security processes and controls. - - b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid. - - c) when the monitoring and measuring shall be performed.	**C**	Yes, Quarterly reviews are conducted, where the performance of ISMS is captured in detail, these metric-based data provide critical information on the performance of the ISMS.

- - d) who shall monitor and measure; - - e) when the results from monitoring and measurement shall be analysed and evaluated; - - f) who shall analyse and evaluate these results. Documented information shall be available as evidence of the results. - - The organisation shall evaluate the information security performance and the effectiveness of the information security management system.		
9.2 - Internal Audit -		
9.2.1 - **Internal Audit General** - The organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organisation's own requirements for its information security management system; and 2) the requirements of this document. - - b) is effectively implemented and maintained.	**C**	Conducted at least annually and all data is recorded. Internal Audit was conducted In January 8, 2026 Verified the Internal audit report.
9.2.2 - **Internal audit programme** - The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits. - - The organisation shall a) define the audit criteria and scope for each audit. - - b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process.	**C**	Yes, the Internal Audit is conducted at least annually, and all the data and the schedule, criteria and scope of the audit is planned suitably. Verified Management Audit Report: The following documents were considered during the audit: 1. ISMS SOA 27001:2022 2. Internal audit report.

- - c) ensure that the results of the audits are reported to relevant management; - - Documented information shall be available as evidence of the implementation of the audit programme(s)and the audit results.		3. ISMS policies and procedures.
9.3 - Management review -		

9.3.1 - General - Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. 9.3.2 - Management review inputs - The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) changes in needs and expectations of interested parties that are relevant to the information security management system; d) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives; e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan; g) opportunities for continual improvement. 9.3.3 - Management review results - The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews.	**C**	Compliance Team is set up and the management review is conducted every quarter. Suggestions for improvements are documented, categorized and worked up on with a focus on the results of the audit, feedback, continual improvement, risk management etc. Management Review Meeting was conducted on January 19, 2026
10 - Improvement -		
10.1 - Continual improvement - The organisation shall continually improve the suitability, adequacy and	**C**	No major findings reported from the recent Internal audit.

effectiveness of the information security management system.		Internal Audit was conducted on January 8, 2026 Verified the Internal audit report.
10.2 - Nonconformity and corrective action - When a nonconformity occurs, the organisation shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f) the nature of the nonconformities and any subsequent actions taken, g) the results of any corrective action.	**C**	Yes, the Organisation has detailed action plan to address non-conformities if it exists.

Annex-A controls – ISO/IEC 27001:2022

VERIFICATION OF DOCUMENTED INFORMATION & RECORDS AS PER STD REQUIREMENT (C- Conformity, NC-Non Conformity, O-Observation, NA-Not Applicable)		
ISO 27001-2022 ISMS Requirements	**C/O/NC/NA**	**Comments**
5 - Organisational Controls -		
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.	**C**	The ISMS Policy is well defined with topic specific policies in place and is communicated to all the stakeholders in the organisation. Verified ISMS Manual Version 1.4 Dated 18 August 2025.
5.2 - Information security roles and responsibilities - Information security roles and responsibilities should be defined and allocated according to the organization needs	**C**	Yes, the IS roles and responsibilities are allocated and are well defined.
5.3 - Segregation of duties - Conflicting duties and conflicting areas of responsibility should be segregated.	**C**	Yes, the areas of responsibilities are segregated and well defined.
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.	**C**	Yes, Management requires all personal to comply with the topic specific policies in ISMS.
5.5 - Contact with Authorities - The organization should establish and maintain contact with relevant authorities.	**C**	Yes, the organisation continues to maintain contact with relevant authorities.
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.	**C**	Yes, the organisation continues to maintain contact with special interest groups and actively takes part in security forums.

5.7 - Threat intelligence - Information relating to information security threats should be collected and analysed to produce threat intelligence.	**C**	Yes, Cyber Crisis Management Policy is in place.
5.8 - Information security in project management - Information security should be integrated into project management.	**C**	Yes, Information Security is integrated into project management.
5.9 - Inventory of information and other associated assets - An inventory of information and other associated assets, including owners, should be developed and maintained.	**C**	Yes, Asset inventory and asset management in place.
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.	**C**	Acceptable usage policy is well defined and covers all the critical information and is documented. Verified Cybersecurity Policy Manual
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.	**C**	Yes, detailed and well-defined policy exists and defines the process of return of assets.
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.	**C**	Yes, Information in the organisation is well classified according to the needs of the organisation based on CIA and other relevant requirements.
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.	**C**	Yes, Asset and information labelling implemented. Asset Management Policy in place and verified.
5.14 - Information Transfer - Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the	**C**	Yes, Information transfer rules, procedures in place

organization and between the organization and other parties.		
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.	**C**	Access control policy is well defined and in place. Verified Cybersecurity Policy Manual
5.16 - Identity Management - The full life cycle of identities should be managed.	**C**	Yes, Identity management is well defined, and its life cycle is managed.
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.	**C**	Yes, Allocation and management of Authentication information is controlled and well defined.
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.	**C**	Yes, Access rights to information are provisioned, reviewed and monitored in accordance with the organisation specific policy.
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.	**C**	Yes, a well detailed process and procedure is implemented.
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.	**C**	Yes, all information security within supplier agreements is addressed.
5.21 - Managing information security in the ICT supply chain - Processes and procedures should be defined and implemented to manage the	**C**	Yes, a well-defined process and procedure is implemented to manage the IS risks associated

information security risks associated with the ICT products and services supply chain.		with ICT products and services supply chain.
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.	**C**	Yes, Change management of supplier in place.
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.	**C**	Yes, cloud security controls are in place.
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	**C**	Yes, Incident management planning and preparation for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities are in place.
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.	**C**	Yes, Information security incidents are assessed, categorized and addressed.
5.26 - Response to information security incidents - Information security incidents should be responded to in accordance with the documented procedures.	**C**	Yes, a response plan to security incidents in place with documented procedures.
5.27 - Learning from information security incidents - Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	**C**	Yes, an incident learning repository is documented and maintained according to the Incident Management Policy.

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.	**C**	Yes, a process to identify, establish and implement procedures for identify, collect and preserve the evidence related to information security events are in place.
5.29 - Information security during disruption - The organization should plan how to maintain information security at an appropriate level during disruption.	**C**	Yes, the organization has a plan to maintain information security at an appropriate level during disruption.
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.	**C**	Yes, ICT readiness is planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. Verified BCP Document.
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.	**C**	Yes, Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements are identified, documented and kept up to date.
5.32 - Intellectual property rights - The organization should implement appropriate procedures to protect intellectual property rights.	**C**	Yes, the organisation has implemented appropriate procedures and measures to protect IP rights.
5.33 - Protection of records - Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	**C**	Yes, the organisation follows a strict procedure to ensure protection of records from loss, destruction, falsification, unauthorized access and unauthorized release.

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.	**C**	Yes, the organization has identified and meets the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
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.	**C**	Yes, the organization manages information security and is implemented to include people, processes and technologies are reviewed independently at planned intervals, or when significant changes occur.
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.	**C**	Yes, in compliance with the organization's information security policy; topic-specific policies, rules and standards are regularly reviewed.
5.37 - Documented operating procedures - Operating procedures for information processing facilities should be documented and made available to personnel who need them.	**C**	Yes, Operating procedures for information processing facilities are documented and made available to personnel who need them.
6 - People Controls -		
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.	**C**	Yes, BGV are carried out on all candidates before joining the organisation on an ongoing basis taking all relevant applicable laws and regulations by an external vendor.

6.2 - Terms and conditions of employment - The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	**C**	Yes, the employment contractual agreements state the personnel's and the organization's responsibilities for information security.
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.	**C**	Yes, Personnel of the organization and relevant interested parties 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.
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.	**C**	Yes, disciplinary process in place and is communicated to all stakeholders/employees in the organisation.
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.	**C**	Yes, Information Security responsibilities and duties that remain valid after termination or change of employment is well defined and enforced.
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.	**C**	Yes, NDAs are signed at the time of on boarding to the organisation. Verified Samples.

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.	**C**	Yes, controls are implemented to ensure security measures when personnel are working remotely.
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.	**C**	Yes, the organization has a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7 - Physical Controls -		
7.1 - Physical security perimeters - Security perimeters should be defined and used to protect areas that contain information and other associated assets.	**C**	Yes, in place and verified.
7.2 - Physical entry - Secure areas should be protected by appropriate entry controls and access points.	**C**	Yes, in place and verified.
7.3 - Securing offices, rooms and facilities - Physical security for offices, rooms and facilities should be designed and implemented.	**C**	Yes, in place and verified.
7.4 - Physical security monitoring - Premises should be continuously monitored for unauthorized physical access.	**C**	Yes, in place and verified.
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.	**C**	Yes, in place and verified.
7.6 - Working in secure areas - Security measures for working in secure areas should be designed and implemented.	**C**	Yes, in place and verified.

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.	**C**	Yes, a well-defined Clear desk and clear screen policy is implemented and enforced,
7.8 - Equipment siting and protection - Equipment should be sited securely and protected.	**C**	Yes, equipment is secured and protected.
7.9 - Security of assets off-premises - Off-site assets should be protected.	**C**	Yes, equipment is secured and protected.
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.	**C**	Yes, in place.
7.11 - Supporting utilities - Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	**C**	Yes, in place.
7.12 - Cabling security - Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	**C**	Yes, in place.
7.13 - Equipment maintenance - Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	**C**	Yes, in place.
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.	**C**	Yes, the organisation has Data Retention and Disposal Policy, and it is enforced well.
8 - Technological Controls -		
8.1 - User endpoint devices - Information stored on, processed by or accessible via user endpoint devices should be protected.	**C**	Yes, Endpoint security is in place and secured.

8.2 - Privileged access rights - The allocation and use of privileged access rights should be restricted and managed.	**C**	Yes, privileged access rights are allocated and managed.
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.	**C**	Yes, access to information is established and well-defined.
8.4 - Access to source code - Read and write access to source code, development tools and software libraries should be appropriately managed.	**NA**	No internal development activities under AudiTree
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.	**C**	Yes, the organisation has Secure authentication technologies and procedures implemented based on information access restrictions and the topic-specific policy on access control.
8.6 - Capacity management - The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	**C**	Yes, Capacity planning and management is reviewed and updated regularly.
8.7 - Protection against malware - Protection against malware should be implemented and supported by appropriate user awareness.	**C**	Yes, awareness training for all users is conducted and the results are documented.
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.	**C**	Yes, the organisation has a well-defined policy to address vulnerabilities, and a regular Penetration testing is conducted internally and externally with an external vendor.
8.9 - Configuration management - Configurations, including security configurations, of hardware, software, services and networks should be	**C**	Yes, the organisation has Configurations, including security configurations, of hardware, software, services and networks

established, documented, implemented, monitored and reviewed.		established, documented, implemented, monitored and reviewed.
8.10 - Information deletion - Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	**C**	Yes, the organisation makes sure with a defined policy for deletion of Information stored in information systems, devices or in any other storage media when no longer required.
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.	**C**	Yes, Data masking is 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.
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.	**C**	Yes, Data leakage prevention measures are applied to systems, networks and any other devices that process, store or transmit sensitive information.
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.	**C**	Yes, Disaster recovery drills are regularly conducted for backup and recovery of data and the results are documented and stored. DR Drill reports verified.
8.14 - Redundancy of information processing facilities - Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	**C**	Yes, Information processing facilities are implemented.
8.15 - Logging - Logs that record activities, exceptions, faults and other relevant events	**C**	Yes, logs are recorded for all activities.

should be produced, stored, protected and analysed.		
8.16 - Monitoring activities - Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	**C**	Yes, all network, systems and applications are monitored, and appropriate action plans are in place.
8.17 - Clock synchronization - The clocks of information processing systems used by the organization should be synchronized to approved time sources.	**C**	Yes, clocks of all information processing systems are synchronised.
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.	**C**	Yes, the organisation ensures the use and control of utility programs and is in accordance with the Acceptable Usage Policy.
8.19 - Installation of software on operational systems - Procedures and measures should be implemented to securely manage software installation of operational systems.	**C**	Yes, the organisation has procedures and measures in place to monitor and securely manage software installation on all its systems.
8.20 - Networks security - Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	**C**	Yes, a policy to ensure networks security is in place and enforced.
8.21 - Security of network services - Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	**C**	Yes, security of network services is in place. Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.
8.22 - Segregation of networks - Groups of information services, users and information systems should be segregated in the organization's networks.	**C**	Yes, information is segregated and classified. Entity ensures that logical access provisioning to critical systems requires approval

		from authorized personnel on an individual need or for a predefined role.
8.23 - Web filtering - Access to external websites should be managed to reduce exposure to malicious content.	**C**	Yes, access to external websites is controlled and managed.
8.24 - Use of cryptography - Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	**C**	Yes, rules for effective use of cryptography are established. Entity has a documented policy to manage encryption and cryptographic protection controls.
8.25 - Secure development life cycle - Rules for the secure development of software and systems should be established and applied.	**NA**	No internal development activities under AudiTree
8.26 - Application security requirements - Information security requirements should be identified, specified and approved when developing or acquiring applications.	**NA**	No internal development activities under AudiTree
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.	**NA**	No internal development activities under AudiTree
8.28 - Secure coding - Secure coding principles should be applied to software development.	**NA**	No internal development activities under AudiTree
8.29 - Security testing in development and acceptance - Security testing processes should be defined and implemented in the development life cycle.	**NA**	No internal development activities under AudiTree
8.30 - Outsourced development - The organization should direct, monitor and review the activities related to outsourced system development.	**NA**	No development activities outsourced to a third party

8.31 - Separation of development, test and production environments - Development, testing and production environments should be separated and secured.	**NA**	No internal development activities under AudiTree
8.32 - Change management - Changes to information processing facilities and information systems should be subject to change management procedures.	**C**	Yes, a change management policy is in place. Verified the Change Management Policy.
8.33 - Test information - Test information should be appropriately selected, protected and managed.	**C**	Yes, organisation has procedure and process in place to appropriately select, protect and manage the Test information. Verified the Change Management Policy.
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.	**C**	Yes, a detailed policy is in place for the Protection of information of systems during testing and audits. The Organisation identifies vulnerabilities on the company platform through an annual penetration testing exercise.

---END OF REPORT---