Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of Controls

For the period, July 01, 2025, to December 31, 2025

SOC2 Type II Report

Attestation and Compliance Services

Compiled by: Satis IT Solutions
www.satisit.com

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

1. Independent Service Auditors' Report

Independent Service Auditors' Report on Description of Karyacloud Ebiz Technologies Private Limited's System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability and Confidentiality trust service criteria.

To the Management of Karyacloud Ebiz Technologies Private Limited

Scope

We have examined Karyacloud Ebiz Technologies Private Limited (the "Service Organization" or "Karyacloud ") accompanying System Description Provided by Service Organization of its system for Software Development Services for the period of July 01, 2025, to December 31, 2025 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description for the period of July 01, 2025, to December 31, 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria *for Security, Availability and Confidentiality (applicable trust services criteria)* set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The Description also indicates that Karyacloud Ebiz Technologies Private Limited's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Karyacloud Ebiz Technologies Private Limited's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Karyacloud Ebiz Technologies Private Limited's responsibilities

Karyacloud Ebiz Technologies Private Limited is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Karyacloud Ebiz Technologies Private Limited has provided the accompanying assertion titled, Karyacloud Ebiz Technologies Private Limited's Management Assertion (Assertion) about the presentation of the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Karyacloud Ebiz Technologies Private Limited is responsible for:(1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's

service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

obtaining an understanding of the system and the service organization's service commitments and system requirements

performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria

performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operated effectively based on the applicable trust services criteria.

testing the operating effectiveness of those controls based on the applicable trust services criteria.

evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Other matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, except for the effects of the matters giving rise to the modification, in all material respects:

a. the Description presents the system that was designed and implemented for the period of July 01, 2025, to December 31, 2025, in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively [and if the subservice organization(s)] and user entities applied the controls assumed in the design of Karyacloud Ebiz Technologies Private Limited's controls for the period of July 01, 2025, to December 31, 2025.

Restricted Use

This report, including the Description of tests of controls and results thereof in Section IV is intended solely for the information and use of Karyacloud Ebiz Technologies Private Limited, user entities of the Service Organization's using the Software Development Services relevant to the Security, Availability and Confidentiality for the period of July 01, 2025, to December 31, 2025, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.
- How the Service Organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how they interact with related controls at the Service Organization to meet the Applicable Trust Services Criteria.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The Applicable Trust Services Criteria.
- The risks that may threaten the achievement of the Applicable Trust Services Criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

For,

TUSHAR S P

License no: 58148
Date: January 23, 2025

SECTION 2

MANAGEMENT ASSERTION PROVIDED BY SERVICE ORGANIZATION

KARYACLOUD EBIZ TECHNOLOGIES PRIVATE LIMITED

(Formerly known as DIVIDANT BUSINESS SOLUTIONS PRIVATE LIMITED)

Management Assertion provided by KARYACLOUD EBIZ TECHNOLOGIES PRIVATE LIMITED.

January 21, 2026

We have prepared the accompanying description of systems in Section 3 of Karyacloud Ebiz Technologies Private Limited (the "Service Organization" or "Karya.cloud") throughout the period July 01, 2025 to December 31, 2025 related to Karya.cloud's SaaS products, that are based on patented AI and Image Recognition technology, provide exceptional speed, accuracy, sales lift, and cost savings to its enterprise customers based on criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("Description Criteria"). The description is intended to provide report users with information about our system used for providing SaaS products, that are based on patented AI and Image Recognition technology, provide exceptional speed, accuracy, sales lift, and cost savings to its enterprise customers., particularly information about system controls that Karya.cloud has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security, Availability, and Confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

Karya.cloud uses GCP (Google Cloud Platform) ("Subservice Organization") as the cloud service provider. The Description includes only the controls of Karya.cloud and excludes controls of Subservice Organization. The Description also indicates that certain trust services criteria specified therein can be met only if the Subservice Organization's controls assumed in the design of Karya.cloud's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the Subservice Organization.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Karya.cloud's controls are suitably designed and operated effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

a) The Description presents the System that was designed and implemented throughout the period July 01, 2025, to December 31, 2025, in accordance with the Description Criteria.

b) The controls stated in the Description were suitably designed and implemented to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Karya.cloud's controls throughout the period July 01, 2025, to December 31, 2025.

For Karyacloud Ebiz Technologies Private Limited

Name: Dhanvi Meda
Designation: CEO &
Product Head Date:
January 21, 2026

SECTION 3

DESCRIPTION OF THE SYSTEM

Karya.Cloud's description of its SaaS Application

Company Background

"Karyacloud Ebiz Technologies Private Limited builds world-class enterprise SaaS platform. Karya.cloud have helped more than 100 service/marketing/consulting/medical organizations improve their business operations through streamlining the processes. We use computer vision technology combined with Artificial intelligence to provide accurate and real-time action-ready insights to managers, owners, sales leaders, category managers, and brand managers to make data-backed decisions and optimize their load and budget across departments."

Description of Services Provided

Karya.cloud SaaS products, that are based on patented AI and Image Recognition technology, provide exceptional speed, accuracy, sales lift, and cost savings to its enterprise customers.

Karya.cloud believes in the power of AI and Image Recognition to free humans of mental and physical drudgery so that they can do more with their time and capital. Hence, Karya.cloud products augment and empower humans in all the industries with automated Image Recognition.

Karya.cloud also believes in making "net-positive" impact on the world and contributing towards environmental sustainability. With this belief, Karya.cloud solves large-scale & systemic problems with real-time & actionable AI solutions.

Components Of the System Used to Provide the Service

System Boundaries

Components of the System

Infrastructure

Primary infrastructure used to provide Karya.cloud's Application Development, Innovative products, Webhosting and client POC's

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Hyper-V Core Terminal Servers	On-Premises Server Hardware (Dell PowerEdge T440)	Used for internal application development and automated testing activities (e.g., Selenium scripting).
Azure Virtual Machine	IaaS – Infrastructure as a Service	Hosts production and staging web applications and backend services.

Azure Storage Account	Cloud Storage (IaaS)	Securely stores application files used by web applications and services.
Google Cloud SQL	PaaS – Platform as a Service	Managed relational database service used for secure data storage and querying by applications.

Software

Primary software used to provide includes the following:

Primary Software	
Software	**Purpose**
.NET Core	Backend application framework used to develop secure, scalable, and cross-platform web services.
C#	Primary programming language used for server-side application development in .NET-based services.
ASP.NET Web API	Framework used to build RESTful APIs that enable secure communication between client applications and backend services.
jQuery	JavaScript library is used to enhance client-side interactivity and improve user experience in web applications.
Cloud SQL (Google / Azure SQL)	Managed relational database platform used for secure data storage, structured querying, and automated maintenance operations.
Azure Containers	Used to deploy and run application components in an isolated, scalable containerized environment without managing underlying servers.
Telerik UI Controls for Web	Third-party UI component library used to provide responsive, accessible, and rich web user interfaces.
React.js	JavaScript framework is used to build dynamic and responsive front-end components for web applications.
Redux	State management library used to maintain predictable and secure data flow in React-based applications.

Ionic Framework	Cross-platform framework used to develop hybrid mobile applications for Android and iOS from a single codebase.
SwiftUI	Native iOS UI framework used to build secure and high-performance mobile applications for Apple devices.

People

The staff can be classified into the following departments:

- The Board: Oversees the organizational direction and decides the strategy for the product and technology.
- Support Services: Human resources, IT & Admin. They assist the organization in ensuring that the delivery activities are smooth.
- AI Delivery and R&D Team: The Karya.cloud Innovation team continuously performs research and proof of concept activities to improve the Karya.cloud Tools and applications to take them to the next level\new features.
- Product Engineering: The software development team that adds features to the product and fixes issues.
- Project Delivery Team: Implements the solution for a new customer, helps in testing upgrades for an existing customer, also configures and customizes the customer based on the need.
- Customer Support Team: 24x7 support for any customer issues, which can range from a query to an unavailability issue
- Product Management: Maintains and owns the product roadmap and functionally directs the product development team.
- Sales / Pre-Sales and Marketing: Scouting for new opportunities, lead generation, product demos, and filling up RFPs.
- IT and Devops Team: Responsible for maintaining local hardware, network and server infrastructure ensuring each user gets smooth services.

Data

The customer shared\approved test data: Karya.cloud tests the client applications on a dev\test environment. It may contain mandatory test inputs based on use cases and data from the customer authorized and approved data.

Processed Data: Karya.cloud team uses the test data, where the client \Karya.cloud hosted test \Dev environment with all required authorized approvals.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Karya.cloud policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Karya.cloud team member.

Physical Security

Physical protection shall be achieved by creating several physical barriers around Karya.cloud premises and information processing facilities. Each barrier should establish a security perimeter, creating a defense in depth strategy and eliminating a single point of failure.

Logical Access

Logical Access controls shall be deployed with the principle of 'deny all unless explicitly permitted' to protect information from unauthorized access. Customers, third-party vendors and service providers shall be provided with access to Karya.cloud information assets only upon presenting business needs and signing the contractual agreement.

Access to this network is protected by user id and password-based access.
For the internal office networks, there is access control via user id and password to various resources.
During the hiring and termination process, HR follows the access activation and deactivation procedure.

Computer Operations - Backups

This procedure applies to all individuals who access, use and control Karya.cloud owned resources. This includes but is limited to Karya.cloud employees, contractors, consultants, and other workers.

The Head of Departments / Business Units shall clearly identify the data to be backup, the minimum backup frequency and archival rules for the respective assets. The IT Department is responsible for the implementation of a Backup plan for the servers.

There is a limited number of people within the organization who could download or restore a particular backup

Computer Operations – Availability

The SAAS services by GCP have a certain reliability which is leveraged for providing the services to our customers.

Since we manually scale Docker containers based on the number of requests, availability may still be affected by usage spikes or performance issues. To mitigate this, we have implemented a high-availability setup with multiple Docker instances and multiple nodes, ensuring the system remains accessible during high demand or performance fluctuations, while continuing to scale containers based on load as needed.

Change Management

This policy establishes a standard procedure for managing change requests in an agile and efficient manner, to drastically minimize the risk and impact on the business operations of the company.

The change in management process begins with the creation of a Change Request within the company's selected technology platform. It ends with the satisfactory implementation of the change and

communication of the result of that change to all interested parties. Further Reporting shall be a part of the entire process, at every step.

Change Management is a continuous improvement within the IT systems of the company, and it generally includes the following steps:

1. Prioritize and respond to the change proposals.
2. Conduct a cost-benefit analysis of the proposed changes.
3. Assessment of risk associated with the changes.
4. Change implementation and monitoring.

Firewalls

Firewalls are in place to ensure that there is no unauthorized access of Organization's resources. The firewalls have monitoring logs, and they are reviewed on a periodic basis.

In addition, remote access is made available via VPN for restricted set of users for a specified time. This set of user access is also reviewed on a periodic basis.

Boundaries of the System

The scope of this report includes the Karya.cloud application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application.

Karya.cloud may depend on a few vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors.

The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

This report does not include the data center hosting services provided by GCP.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication and Monitoring

Control Environment

Integrity and Ethical Values

Integrity and ethical values, while they are not something that can be enforced via policy documents, can be promoted by creating an environment and culture that makes it easier to have integrity and be ethical than not.

Employees undergo training related to expected standards of behavior and ethics, they are also asked to go through policy documents related to ethics and integrity during their orientation.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgement form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

An annual performance appraisal is held for all employees, which is based on a points system.

The employees are encouraged to improve their skills and be more productive. Pay revisions and compensation improvements and promotions are linked to the performance appraisal.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for specific jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Management philosophy for the organization is based on the premise that focusing on the customer's long term needs rather than providing short term solutions is a more beneficial policy in the long run.

In addition, management believes that the changing regulatory environment as well as improvements in technology provide business opportunities, so it is important to stay up to date on these must be looked at as opportunities rather than problems.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Karya.cloud organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

The goal of the organization is to have lean and agile teams. However, every team member is part of a formal hierarchy that rolls up to the CEO.

While employees and multiple teams may collaborate informally to get things done faster, in case of conflicts or deciding how something new would be handled, the formal hierarchy is used as the basis for coming to conclusions.

It is also ensured that collaborative work does not mean sharing confidential data or credentials that must not be shared with unauthorized people.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

The human resource department under the direction of the board and the leadership directs the policies and procedures such that there are:

- Delivery excellence

- an environment where merit and performance are valued.
- People feel part of something bigger than them.
- a high-performance work ethic

There are policies that dictate induction of new joiners, exit and termination policies as well as promotions that lead to achieving the goals listed above.

Risk Assessment

Karya.cloud assessment process identifies and manages risks that could potentially affect Karya.cloud ability to provide reliable services to its customers. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. The Karya.cloud identifies the underlying sources of risk, measures the impact on the organization, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Karya.cloud management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment and critical staff
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance - legal and regulatory changes

Karya.cloud has established an internal team responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. Karya.cloud attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Information and Communications Systems

It is important for the customer and internal stakeholders to be aware of the changes to be made to the production systems as well as the reasons for that. The same applies to communications after the changes have been made or rolled back.

Similarly, a new initiative taken internally to add product features or to improve the systems in any other way needs to be communicated to the team and responsibilities need to be assigned. That requires a robust and efficient mode of communication that is also secure.

Various degrees and means of communication are required for interaction with prospects, live customers and employees.

In addition, it is required to keep track of communications as well as what actions have been taken to achieve the goals.

Monitoring Controls

Being a cloud-based system, the monitoring is via logs, which may be application logs as well as access logs.

A dedicated support team monitors all the production systems 24 x 7 and keeps an eye out for anomalies.

The support team also receives issues raised by the customer and attempts to correlate the customer's findings with the corresponding logs, thereby pre-empting a customer report by taking corrective action even before it is reported by them.

Log monitoring is also used to pass on valuable information to the development teams to solve issues that cannot be simulated in a development environment.

On-Going Monitoring

Karya.cloud management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Karya.cloud operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Karya.cloud personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System Since the Last Review

Since the organization's last review, no significant changes have occurred to the services provided to user entities.

Incidents Since the Last Review

Since the organization's last review, no significant incidents have occurred with the services provided to user entities.

Applicable Trust Service Criteria and Related Controls

The security, availability and confidentiality trust services categories and Karya.cloud related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and

Results". Karya.cloud has determined that Processing Integrity and Privacy trust services Categories are not relevant to the system.

Subservice Organizations

This report does not include the data center hosting services provided by GCP at multiple facilities.

Subservice Description of Services

The SAAS services provided by GCP are monitored by management; however, they have not been included in the scope of this review.

Complementary Organization Controls

Karya.cloud services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to Karya.cloud services to be solely achieved by Karya.cloud control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Karya.cloud.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization		
Category	**Criteria**	**Applicable Controls**
Common Criteria/ Security	CC6.4	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 60 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Karya.cloud management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Karya.cloud performs monitoring of the subservice organization controls, including the following procedures.

- Reviewing attestation reports on services provided by vendors and subservice organizations.

Complementary Customer Control (CUEC)

Karya.cloud controls related to Karya.cloud cover a subset of overall internal control for each user of the software application. The control objectives related to Karya.cloud cannot be achieved solely by the controls put in place by Karya.cloud, each customer's internal control needs to be considered along with Karya.cloud's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Complementary Customer Controls (CUECs)	
Related Criteria	**CUEC Description**
CC5.1 CC5.2 CC5.3 CC6.1	Customers are responsible for managing their organization's Karya.cloud software application account as well as establishing any customized security solutions or automated processes using setup features
CC5.2 CC6.3	Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Karya.cloud software application account
CC7.2 CC7.3 CC7.4	Customers are responsible for notifying Karya.cloud of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Karya.cloud software application.
CC8.1	Customers are responsible for any changes made to user and organization data stored within the Karya.cloud software application.
CC7.2 CC7.3 CC7.4	Customers are responsible for communicating relevant security and availability issues and incidents to Karya.cloud through identified channels.

SECTION 4

TESTING MATRICES

Trust Services Criteria and Description of Related Controls:

Ref	Control Short	Controls Implemented by Entity	Test Procedures	Results of the Test
1	**Control Environment:**			
CC1.1	**Integrity and Ethics: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**			
	Mission and Vision Statements	The Company has established formal mission and vision statements that define its strategic direction. In addition, the Company has developed and communicated a clearly articulated statement of ethical values, which is understood and acknowledged across all levels of the organization.	Inspected the Company's documented mission and vision statements to verify that they have been formally established. Reviewed the Company's documented statement of ethical values to confirm that it has been developed and communicated within the organization.	No Exceptions Noted
	Whistle Blower Policy	The Company has implemented a formal whistle blower program designed to provide employees and stakeholders with a mechanism to report concerns related to financial irregularities, unethical practices, or potential fraud. The program is supported by a documented policy that outlines the reporting channels, protections against retaliation, and the process for investigating reported concerns.	Inspected the Company's whistle blower policy to verify that it has been formally documented and approved. Reviewed the policy to confirm that it establishes reporting mechanisms, defines protections for whistle blowers, and outlines procedures for addressing reported concerns.	No Exceptions Noted
	Code of Conduct	The Company has established a formal Code of Conduct policy, documented within the Employee Handbook, which defines standards and guidelines for ethical behaviour expected from all personnel. The Code of Conduct includes provisions related to security and privacy requirements. Employees are required to	Inspected the Company's Code of Conduct policy to verify that standards and guidelines for ethical behaviour have been formally documented, including security and privacy requirements. Reviewed the Employee Handbook to confirm inclusion of the Code of Conduct provisions.	No Exceptions Noted

		review and formally acknowledge their understanding and acceptance of the Code of Conduct as part of their onboarding and ongoing compliance responsibilities.		
	Signed NDA	The Company requires all new employees to review and sign a Confidentiality Agreement/Non-Disclosure Agreement (NDA) as part of the onboarding process. The NDA establishes the employee's responsibility to protect the confidentiality of Company and client information and outlines restrictions on unauthorized use or disclosure. Signed agreements are maintained in the employee's personnel file or other designated repository.	Selected a sample of recently onboarded employees. Inspected the corresponding personnel files to verify that signed Confidentiality Agreements/NDAs were obtained and retained. Confirmed that the NDA terms address the safeguarding of Company and client confidential information.	No Exceptions Noted
	Acceptable Use Policy	As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of the Acceptable Use Policy (AUP).	Selected a sample of new joiners and inspected the acknowledgement from them of the Acceptable Use Policy	No Exceptions Noted
	Security Certifications	The Company has obtained industry-recognized security certifications to demonstrate its commitment to maintaining effective information security practices. The Company currently holds the ISO 27001, PCI-DSS certification, which establishes requirements for implementing, maintaining, and continually improving its Information Security Management System (ISMS).	Inspected the Company's ISO 27001, PCI-DSS certification to verify that it is valid and current. Reviewed the certification details (e.g., certificate number, issuing body, scope, and validity period) to confirm authenticity and alignment with the Company's operations.	No Exceptions Noted
CC1.2	**Board Oversight: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**			

	Management Review Meetings (MRM)	The Company conducts Management Review Meetings (MRMs) on a semi-annual basis to evaluate the overall security posture, review changes in the environment, discuss emerging technology trends, assess the occurrence of security incidents, and plan security-related initiatives. The meetings ensure that management maintains oversight of the information security program and its alignment with organizational objectives.	Inspected the calendar invites for Management Review Meetings to verify that MRMs were scheduled and conducted on a periodic basis.	No Exceptions Noted
	Business Meetings	The Company's management team conducts Monthly meetings to discuss business operations, review operational issues, and address strategic and tactical decisions. These meetings facilitate ongoing oversight and coordination of organizational activities.	Inspected calendar invites or schedules for management meetings to verify that meetings are held on a recurring basis.	No Exceptions Noted
CC1.3	**Management Structures: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**			
	Organisation Charts	The Company has established organization charts that depict authority, reporting lines, and responsibilities for the management of its information systems. The organization charts are communicated to employees and updated as necessary to reflect changes in roles or reporting structures.	Inspected the organization chart to gain an understanding of the hierarchy and reporting lines. Inquired with management to confirm that organization charts are maintained and updated periodically to reflect organizational changes.	No Exceptions Noted
	ISMS Policies	The Company has established Information Security Management System (ISMS) policies and related IT procedures that define its information security processes, practices, and organizational responsibilities.	Inspected the ISMS manual and related IT policies to verify that they are formally documented. Reviewed the documentation to ensure it adequately describes the Company's information	No Exceptions Noted

			security processes, practices, and organizational responsibilities.	
	Approval of ISMS Policies	The Company's Information Security Policy and related procedures, including those applicable to HR processes, are reviewed and approved by management at least annually. The approval process ensures that all policies remain current, relevant, and aligned with organizational objectives and regulatory requirements.	Inspected the ISMS manual and related IT policies to verify that any changes made during the audit period were formally documented. Confirmed that updates or revisions were reviewed and approved by the appropriate management authority.	No Exceptions Noted
	Roles and Responsibilities	The Company has established information security policies and procedures that clearly define roles and responsibilities for managing information security processes and practices. These policies outline accountability for safeguarding information assets, implementing controls, and ensuring compliance with organizational and regulatory requirements.	Inspected the information security policies and procedures to verify that roles and responsibilities are formally documented. Reviewed the documentation to confirm that responsibilities for information security processes and practices are clearly assigned and communicated to relevant personnel.	No Exceptions Noted
CC1.4	**Attract and Retain Talent: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**			
	HR Policies	The Company has documented HR policies and procedures that cover recruitment, training, onboarding, and exit processes. These policies define the responsibilities and processes to ensure consistent and compliant management of human resources throughout the employee lifecycle.	Inspected the HR policies and procedures to verify that they are formally documented. Reviewed the documentation to confirm coverage of recruitment, training, onboarding, and exit processes.	No Exceptions Noted
	Job Descriptions (JD) in Place	The Company maintains documented job descriptions for all roles, specifying the requirements, responsibilities, and	Inspected the HR policies and relevant job descriptions to verify that role requirements and responsibilities are formally documented.	No Exceptions Noted

		competencies needed for each position. Candidates' qualifications and abilities are evaluated against these requirements as part of the hiring or internal transfer process to ensure suitability for the role.	Reviewed supporting evidence to confirm that candidates' abilities are evaluated against the documented requirements during hiring or internal transfer processes.	
	Offer letter & Appointment letter	The Organization requires all new employees to sign an offer letter and appointment letter as acknowledgment and acceptance of the terms of employment. These documents outline the employee's position, responsibilities, and other employment terms, serving as formal agreement between the Organization and the employee.	Inspected the offer letters and appointment letters for new employees to verify that they are formally documented. Reviewed the signed documents to confirm that new employees have accepted the terms of employment, including role and responsibilities.	No Exceptions Noted
	External BGV	The Organization engages external third-party vendors to perform background verification checks for experienced new hires. These checks include education qualification verification, employment history verification, address verification, and, where necessary, criminal record checks.	Inspected the background verification reports maintained by the HR department to verify that external background checks were conducted for experienced new hires.	No Exceptions Noted
	Security Awareness Training	The Organization provides security awareness training as part of the new hire induction program. The training covers information security policies, physical access controls, HR security policies, and the procedures for identifying and reporting security incidents. All new employees are required to attend this training to ensure awareness of their security responsibilities.	Inspected the new hire induction training materials to verify that security awareness topics, including relevant policies and procedures for reporting security incidents, are covered. Reviewed attendance records maintained by HR to confirm that new employees have completed the security awareness training as part of their induction.	No Exceptions Noted

	Laptop provision for new joiners	The Organization provisions laptops and other necessary equipment for new employees in accordance with standard onboarding procedures, including scenarios where employees work from home or during extended business disruptions.	Reviewed the HR policies and procedures to confirm that laptop provisioning and new joiner onboarding processes are defined. Inspected records of new joiner equipment provisioning to verify adherence to the defined process.	No Exceptions Noted
CC1.5	**Accountability: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**			
	Roles and Responsibilities	The Organization defines roles and responsibilities in written job descriptions and communicates them to employees and their managers. This ensures clarity of accountability and supports effective management of organizational and IT responsibilities.	Inspected IT policies and the roles and responsibilities documentation to verify that responsibilities are formally defined and communicated.	No Exceptions Noted
	Job Descriptions	The Organization maintains job descriptions for all roles, which are reviewed and updated by management annually or as required to reflect changes in responsibilities, skills, or performance expectations.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as an when required.	No Exceptions Noted
	Annual Code of Conduct Sign off	he Organization requires all employees and contractors to acknowledge the Code of Conduct on an annual basis. This ensures ongoing awareness and adherence to ethical standards and organizational policies.	Reviewed records maintained by HR or the compliance system to verify that all employees and contractors have acknowledged the Code of Conduct during the Audit period.	No Exceptions Noted
	Performance Appraisals	The Organization conducts performance appraisals for all employees at least annually. These appraisals assess employee performance, support	Reviewed performance appraisal records maintained by HR to confirm that appraisals are conducted for all employees at least annually.	No Exceptions Noted

		professional development, and inform role and compensation decisions.		
2	**Communication and Information:**			
CC2.1	**Internal Communication and Information: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**			
	Periodic Business Meetings	The Organization conducts standing Quarterly departmental meetings to discuss operational matters, review status updates, and ensure alignment across teams.	Inspected meeting calendar invites or schedules to verify that departmental meetings are conducted.	No Exceptions Noted
CC2.2	**Internal Communication: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**			
	Network Diagram	The Organization has documented system boundaries, including logical and physical boundaries. Network diagrams cover networking devices such as routers, firewalls, switches, and servers, including wireless infrastructure.	Reviewed system and network diagrams to confirm that the Organization has documented the logical and physical boundaries of its IT environment.	No Exceptions Noted
	Security policies on Intranet	The Organization publishes IT and information security policies on its SharePoint site to ensure accessibility to internal personnel	Inspected the SharePoint site to verify that IT security policies are available and accessible to internal users.	No Exceptions Noted
	Incident Management	The Organization maintains an enterprise-wide incident management process to identify, respond to, and remediate information security and operational incidents.	Inspected the ISMS and information security policies to confirm that the incident management process is formally documented.	No Exceptions Noted
	Client Escalation Matrix	The Organization maintains a client-specific escalation matrix to ensure timely communication with external clients regarding incidents or issues. Project	Reviewed the client-specific escalation procedures to verify that they are formally documented and established for timely communication.	No Exceptions Noted

		Managers or IT management follow the defined procedures for escalation.	Confirmed that the procedures designate appropriate escalation points and responsibilities.	
CC2.3	**External Communication: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**			
	Client Contracts with Confidentiality Clause	The Organization includes commitments related to security, availability, and confidentiality of its systems in client contracts, statements of work (SOWs), and service level agreements (SLAs). These clauses define the Organization's obligations to safeguard client data and maintain service reliability.	Inspected client contracts, SOWs, and SLAs to verify that terms related to security, availability, and confidentiality of services are included.	No Exceptions Noted
	Customer SLA monitoring	The Organization monitors customer-specific SLAs on a daily, weekly, and monthly basis, as required by client agreements. SLA results are shared with customers according to their contractual requirements.	Inspected SLA reports and dashboards maintained by the Organization to verify that SLA performance is monitored at the defined intervals. Reviewed documentation to confirm that SLA performance information is communicated to customers in accordance with contractual requirements.	No Exceptions Noted
	Customer responsibilities in client contracts	The Organization documents customer responsibilities in client contracts and system documentation. This ensures clarity of roles and responsibilities between the Organization and its clients.	Inspected sample customer SOWs and contracts to verify that customer responsibilities are clearly defined. Reviewed associated system documentation to confirm that roles and responsibilities are consistently communicated.	No Exceptions Noted
	Reporting of incidents to external users	The Organization communicates incidents that impact external users via email or	Reviewed incident reports and emails to external users to verify that major incidents are	No Exceptions Noted

		other official channels. The incident response plan and incident management policy define incident types and provide guidance on when and how to report incidents to external parties. Root cause analysis is provided when required.	communicated appropriately. Confirmed that, where required, root cause analyses were provided along with the incident notifications.	
3	**Risk Assessment:**			
CC3.1	**Business Objectives: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**			
	Business Plans	Management has regular business planning process in place that examines existing objectives and establishes new objectives when necessary. Related business risks are discussed in such meetings.	Inspected a sample of business meeting minutes to determine that business meetings are held to discuss medium term and long-term business goals and related risks. Inspected a copy of the annual board meeting presentation (containing annual, medium-term plans) done by Senior management to determine that strategic plans / business objectives are in place	No Exceptions Noted
CC3.2	**Risk Assessments: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.**			
	Risk Assessment	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
	Rating of Risks	Identified risks are rated and get prioritized based on their likelihood, impact, detection and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No Exceptions Noted

CC3.3	**Fraud Risk: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**			
	Patch Management	The Organization uses Seqrite Endpoint Protection to manage and deploy patches to user systems. The solution ensures that operating systems and critical applications are updated periodically, helping to mitigate vulnerabilities and maintain the security posture of the IT environment.	Inspected screenshots and logs from Seqrite Endpoint Protection to verify that patches are applied periodically to user systems.	No Exceptions Noted
	Risk Management Policy	Company has defined a formal risk management process for evaluating risks based on identified vulnerabilities, threats, asset value and mitigating controls.	Inspected Risk Assessment policy and process to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
CC3.4	**Changes to Systems and Risks: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**			
	Risk Assessment	Emerging technology and system changes are considered when performing risk assessment	Inspected sample of Risk Assessment performed during the audit period to determine that risk assessment is carried out for emerging technology and system changes.	No Exceptions Noted
4	**Monitoring Activities:**			
CC4.1	**Evaluation of Internal Controls: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**			
	Internal Audits	The Organization's internal audit function conducts periodic reviews of system security, including assessments of controls, processes, and compliance with policies. Results of the audits, along with recommendations for improvement, are reported to management to facilitate corrective actions.	Inspected internal audit reports and supporting documentation to verify that system security reviews are conducted periodically. Reviewed evidence of corrective actions taken in response to audit findings to confirm that management addresses recommendations appropriately.	No Exceptions Noted

	System Access reviews	The Organization performs regular reviews of IT system access rights on a monthly basis. These reviews ensure that access privileges are appropriate, aligned with job responsibilities, and reconciled. Access control policies document the process for granting, modifying, and revoking system access.	Inspected the information security policies containing access controls to determine that these are documented. Inspected a sample of system access review reports to determine that access rights are reviewed regularly and user access lists are reconciled against active HR records.	No Exceptions Noted
CC4.2	**Internal Control Deficiencies: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**			
	Firewall logs	The Organization's firewalls are configured to capture and log network events. These logs provide visibility into network activity and support monitoring, investigation, and management of security incidents.	Inspected the firewall configuration settings to verify that event logging is enabled and operational.	No Exceptions Noted
	Vulnerability Assessment & Penetration Testing (VAPT)	The Organization engages a third-party service provider to conduct vulnerability assessments and penetration tests on an annual basis. The assessments identify potential weaknesses in systems and networks, and corrective actions are implemented to remediate identified vulnerabilities.	Inspected the latest vulnerability assessment and penetration test reports to verify that assessments are performed periodically by a third party.	No Exceptions Noted
	VAPT Review	Management reviews the results of vulnerability assessments and penetration tests to ensure timely remediation of identified weaknesses and to maintain the security posture of the Organization.	Reviewed the latest vulnerability assessment and penetration test reports to verify that results are formally reviewed by management. Confirmed that identified vulnerabilities have been remediated in accordance with management's review and approval process.	No Exceptions Noted

5	Control Activities:			
CC5.1	**Risk Mitigation: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**			
	Segregation of duties	The Organization enforces segregation of duties for critical functions and key departments to reduce the risk of errors, fraud, or unauthorized activity. Roles and responsibilities are clearly defined in policies and procedures to ensure that no single individual has conflicting responsibilities over key processes or systems.	Reviewed documentation to confirm that responsibilities for critical functions are appropriately segregated to mitigate risks.	No Exceptions Noted
CC5.2	**General Controls over Technology: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**			
	Endpoint protection for WFH Staff	The Organization implements comprehensive information security measures using Seqrite Endpoint Protection to secure endpoints and prevent data leakage for personnel working remotely or from home. These measures include deployment of endpoint protection tools, data loss prevention controls, and monitoring mechanisms. The effectiveness of these controls is reviewed or audited at least quarterly to ensure continued protection.	Inspected logs, screenshots, and configuration records from Seqrite Endpoint Protection to verify that endpoint protection and data leakage prevention measures are applied for remote and WFH personnel.	No Exceptions Noted
CC5.3	**Policies and Procedures: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**			

	Policies and procedures for major functions	The Organization has implemented documented policies and standard operating procedures (SOPs) across its major business and operational functions. These policies and procedures define roles, responsibilities, and standardized processes to ensure consistent and controlled operations.	Inspected the list of policies and procedures maintained by the Organization to verify that major business functions have formally documented and approved policies and SOPs. Reviewed the documentation to confirm that the policies and procedures cover key operational and business processes and are communicated to relevant personnel.	No Exceptions Noted
6	**Logical and Physical Access Controls:**			
CC6.1	**Logical Access: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.**			
	Access Management Policy	The Organization has documented procedures for logical access management. These procedures define how access to systems and information is granted, modified, and revoked in accordance with security requirements and organizational policies.	Inspected the access control policy and procedure documentation to verify that logical access controls are formally defined.	No Exceptions Noted
	Access Management Least Privileges	The Organization grants system access on a least privilege basis by default. Any additional access rights require formal approval from the appropriate authority to ensure that users have only the access necessary to perform their roles.	Reviewed access control procedures to confirm that least privilege principles are enforced and that additional access requires proper approval.	No Exceptions Noted
	Hardening standards	The Organization has established hardening standards for End User systems and office infrastructure. These standards include security group configurations, access control settings, system configuration baselines, and standardized policies to secure the IT environment.	Enquired with IT Team that hardening standards are configured and implemented for End User systems and office infrastructure.	No Exceptions Noted

	Active Directory	Infrastructure components and software are integrated with Active Directory (AD) and group policies to enforce authentication and access control across the Organization's IT environment.	Inspected AD and group policy configurations to confirm authentication is enforced through Active Directory. Observed user sign-on procedures to verify that user IDs and passwords are required for access.	No Exceptions Noted
	Remote working policy	The Organization has a documented remote working policy that governs external access, including work-from-home scenarios during business disruptions. By default, external access by employees is prohibited unless explicitly approved.	Reviewed the remote working policy to confirm it covers WFH procedures and external access guidelines. Enquired with IT staff and verified that external access is restricted by default.	No Exceptions Noted
	Software List	The IT department maintains an up-to-date inventory of all software installed within the Organization to ensure proper licensing, updates, and patching.	Reviewed the software inventory maintained by IT to verify it is current. Inspected sample Systems to confirm that software versions are up to date.	No Exceptions Noted
	Asset Register	The Organization maintains an inventory of internal and external information assets. Each asset is assigned an owner responsible for evaluating access rights based on job roles. Criticality ratings are defined for all assets.	Reviewed the asset register to verify that all assets and their owners are clearly documented.	No Exceptions Noted
	Password policy in AD	The Organization enforces the following password parameters for Active Directory accounts: Minimum length of 8 characters Complexity enabled Password history set to 12	Inspected default password security settings in domain group policy to confirm that the above parameters are enforced.	No Exceptions Noted

	Classification of Data	All confidential data is classified according to the Organization's data classification policy. This classification guides access, handling, and protection measures.	Inspected the information security policies to verify that data classification procedures are documented and implemented.	No Exceptions Noted
CC6.2	**Granting Logical Access: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**			
	Email from HR to IT for Joiners and Leavers	On the day of joining, HR notifies the IT Helpdesk via email with the details of new employees. IT then provides the necessary system and application access in accordance with the access management procedures. For employees leaving the Organization, IT deactivates accounts based on written access revocation requests sent by HR. All provisioning and deprovisioning actions are performed only against formal authorization.	Inspected the access control procedures to verify that user access is granted, modified, or deactivated only against written authorization. Reviewed emails and access request forms for selected employees to confirm that written authorization exists for account creation and modifications. Reviewed access revocation requests and exit checklists for selected employees to verify that deactivation actions are formally authorized.	No Exceptions Noted
	Access Revocation	When employees exit the Organization, access to client systems is revoked by notifying the client manager via email to ensure timely removal of user privileges.	Reviewed access revocation emails sent to clients to verify that clients are informed of employee exits in a timely manner.	No Exceptions Noted
	Exit Formalities	Upon employee termination, the manager initiates the formal exit process. HR notifies relevant teams, including IT, within 24 hours to deactivate or delete the employee's accounts from email systems and applications. An exit checklist is used to ensure compliance with termination procedures.	Reviewed emails from HR to IT and exit checklists for selected exited employees to confirm that the exit process and account deactivation were performed according to defined procedures. Verified in Active Directory or other systems that the user accounts for exited employees are in a disabled status.	No Exceptions Noted

	User deactivation email	HR sends a user deactivation list to IT within 24 hours of employee termination or the last working day. IT deactivates accounts promptly to prevent unauthorized access.	Inspected HR emails to IT for user deactivation for selected off-boarded employees. Verified in Active Directory that the terminated employees' accounts were disabled as per the notification.	No Exceptions Noted
CC6.3	**Revoking or modifying Logical Access: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.**			
	Role based access	The Organization implements role-based security in Active Directory, defining security groups and roles aligned with job requirements. Access rights are assigned based on departmental responsibilities and functional roles to enforce least privilege and segregation of duties.	Inspected Active Directory security groups to verify that roles and groups have been defined according to job functions and departmental requirements.	No Exceptions Noted
CC6.4	**Physical Access: The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**			
	Office Entry is restricted	The Organization restricts entry to all premises to authorized personnel, including delivery and loading areas. A physical access control system, including biometric authentication, is implemented to secure the facilities.	Observed that entry points to the premises are secured using a biometric access system. Verified that users enter and exit the premises only after successful authentication through the physical access system.	No Exceptions Noted
	CCTV	Physical access to office premises is monitored through CCTV installed at key points within the premises.	Observed that CCTV cameras are operational and located at strategic locations to monitor entry, exit, and critical areas.	No Exceptions Noted
	Security Guard	A security desk is maintained at office entry points, staffed by trained security personnel who screen employees and visitors before granting access.	Physically observed security personnel at the reception ensuring that all employees and visitors are screened before entering the premises.	No Exceptions Noted

	Visitor Management	All visitors are required to log their details in the visitor register. Visitor badges are issued for identification purposes only and do not provide access to secured areas. Visitors must be escorted by an authorized Organization employee while on the premises.	Inspected the visitor register for selected dates to verify that visitor details are recorded. Physically observed that visitor badges are used solely for identification. Confirmed that visitors are escorted by Organization personnel at all times.	No Exceptions Noted
	Employee picture ID cards	All employees must wear ID cards with photographs at all times while accessing or leaving the facility to ensure proper identification.	Physically observed a sample of employees to confirm compliance with the ID card policy.	No Exceptions Noted
	Physical Access Setup by HR	HR sets up physical access for new employees after completion of onboarding formalities. By default, access to sensitive areas is restricted until specifically authorized.	Inspected a sample of new employees to confirm that access rights were granted only after HR onboarding formalities and only to authorized personnel.	No Exceptions Noted
	Physical Access to Server/Network Room and Sensitive Areas	Access to server/network rooms and other sensitive areas is restricted to privileged personnel (IT team). Access is granted only via written approval by the management.	Inquired with IT staff to confirm that access to sensitive areas is restricted to authorized personnel. Inspected a sample of physical access review reports to verify periodic reviews against active employee lists.	No Exceptions Noted
	Revocation of Physical Access	Upon employee termination, HR sends a request to deactivate physical access. Access is revoked by the Admin Team, and employees are required to return ID cards.	Inspected biometric system logs to confirm that terminated employees' access rights were removed. Reviewed exit checklists to verify that ID cards were returned and deactivated.	No Exceptions Noted
	Physical access review periodically	Physical access rights are reviewed quarterly by Internal Audit or HR to ensure that terminated employees no longer have access to facilities.	Inspected a sample of quarterly physical access review reports to verify that reconciliations are performed regularly.	No Exceptions Noted

CC6.5	**Media Handling: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.**			
	Media Handling policy	The Organization has implemented a documented Media Handling Policy that governs procedures for managing, storing, and securing information assets and IT equipment. This policy ensures that all media containing sensitive information is handled in a controlled manner throughout its lifecycle.	Inspected the Media Handling Policy to confirm that procedures for secure handling, storage, and management of information assets and equipment are documented and approved.	No Exceptions Noted
	Media Reuse / Disposal	All media, including laptops and other IT assets, are securely erased before being formatted and reused. Assets that are out of warranty or deemed problematic are stored with the IT department for controlled handling. Currently, there is no disposal of media; only secure reuse is performed.	Reviewed the Media Handling Policy to confirm that procedures require secure erasure of data prior to reuse. Inspected IT records to verify that out-of-warranty or problematic systems are securely stored with IT staff and are not in active use. Verified that no media disposal occurred during the audit period and that all reuse activities follow documented procedures.	No Exceptions Noted
CC6.6	**Network Security: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**			
	Firewall installation	The Organization protects external connectivity points to its office network with a firewall. The firewall provides Unified Threat Management (UTM) services, including intrusion prevention, web filtering, and inbound/outbound traffic control, to safeguard the network from unauthorized access and threats.	Observed the firewall device installed within the office network. Reviewed firewall console settings, including port rules, incoming connection types, whitelisted IPs, and traffic policies, to verify compliance with organizational policies and that connections are allowed only from authorized IPs.	No Exceptions Noted
	Content Filtering	The Organization implements content filtering through the firewall to block access to unauthorized websites, including personal email and storage sites, thereby enforcing acceptable use of the network.	Reviewed firewall configuration for content filtering to verify that access to restricted websites is appropriately blocked.	No Exceptions Noted

	Firewall admin access	Modification of firewall rules is restricted to authorized personnel within the IT team to prevent unauthorized changes to network security configurations.	Inspected the list of users with firewall administrative access to confirm that only authorized IT personnel can modify firewall rules.	No Exceptions Noted
	Removable media prohibited	The use of removable media is prohibited by policy unless explicitly authorized by management. This prevents unauthorized copying or transfer of organizational data.	Reviewed domain policies governing removable media usage. Observed a sample of workstations to confirm that USB devices are not read or used without authorization.	No Exceptions Noted
CC6.7	**Encryption Controls: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.**			
	Encryption Policy	The Organization prohibits the transmission of sensitive information over the Internet or other public communication channels unless such information is encrypted. This ensures the confidentiality and integrity of sensitive data during transit.	Reviewed the Organization's information security policies to confirm that transmission of sensitive information over public networks is permitted only when encrypted.	No Exceptions Noted
	Data Loss Prevention (DLP) Software	The Organization uses DLP software to monitor and prevent unauthorized transmission of sensitive information over public communication paths. The DLP system scans outgoing transmissions and blocks any attempts to send sensitive data in violation of policy.	Enquired with management and reviewed system documentation to confirm that the DLP software scans outgoing transmissions and prevents unauthorized sharing of sensitive information.	No Exceptions Noted
	Removable media prohibited	The Organization prohibits the use of removable media, such as USB drives, unless explicitly authorized by management, to prevent unauthorized copying or transfer of sensitive information.	Reviewed domain policies governing the use of removable media. Observed a sample of workstations to confirm that unauthorized USB devices are not accessed or read.	No Exceptions Noted
CC6.8	**Malicious software and Vulnerabilities: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**			

	Antivirus Installed	The Organization installs antivirus software on all workstations, laptops, and servers. The antivirus system provides malware scanning, email scanning, content filtering, and endpoint protection to prevent, detect, and respond to security threats.	Inspected a sample of desktops, laptops, and servers to confirm that antivirus software is installed. Reviewed the antivirus/firewall console for configuration details related to updates, alerts, and overall system compliance.	No Exceptions Noted
	Regular Update of AV Definitions	Antivirus signature files are updated daily. The antivirus console generates compliance reports to identify any systems with outdated definitions, ensuring continuous protection.	Reviewed console query reports to confirm that all systems had up-to-date antivirus definitions. Verified console configuration for automatic updates and alerting.	No Exceptions Noted
	Local admin access	The ability to install software on workstations and laptops is restricted to authorized IT support personnel through domain policies. Local administrator privileges are granted only on a need-based approval from the Management and Business justification.	Reviewed the Organization's Information Security Policies to confirm that standard users are not permitted to install software. Inspected domain policies to verify that local administrator privileges are disabled for standard users and granted only as per approval procedures.	No Exceptions Noted
	Reporting of virus detected	Any virus or malware detected is reported to the IT team, either automatically by the antivirus system or manually by affected employees, to ensure timely remediation.	Reviewed the antivirus/firewall console to verify configuration for alerting and reporting of virus detections. Examined security training materials to confirm that employees are instructed on reporting virus or malware incidents	No Exceptions Noted
7	**System Operations:**			
CC7.1	**System Operations: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.**			

	Monitor infrastructure and software	The Organization monitors its IT infrastructure and software for noncompliance with internal standards or regulatory requirements that could impact the achievement of business objectives. This ensures that potential threats to system integrity and security are identified and addressed promptly.	Enquired with management and IT staff to confirm that noncompliance with infrastructure and software standards are tracked, reported, and reviewed periodically.	No Exceptions Noted
	Penetration Testing	The Organization conducts periodic penetration testing to identify and remediate vulnerabilities within its systems, applications, and network infrastructure.	Inspected the most recent penetration testing report to verify that testing is performed periodically and that identified issues are documented for remediation.	No Exceptions Noted
	VAPT	The Organization conducts technical vulnerability assessments and penetration testing on a periodic basis. Identified vulnerabilities, especially critical ones, are tracked and remediated in a timely manner to maintain system security and integrity.	Reviewed a sample of vulnerability assessment and penetration testing reports to confirm that scans and tests were performed periodically. Verified that identified vulnerabilities were documented and remediated promptly.	No Exceptions Noted
CC7.2	**Monitor events and attacks: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analysed to determine whether they represent security events.**			
	Alerts from firewall for suspicious activity	The Organization's firewall monitoring system detects suspicious activity on the corporate network and generates alerts for the IT team. These alerts are reviewed and responded to promptly to maintain network security.	Reviewed firewall configuration and alert settings to confirm that suspicious activity triggers notifications to the IT team.	No Exceptions Noted

	IT Help desk support	The Organization maintains an IT helpdesk to handle user requests, including password resets, software issues, and other IT support needs. Requests are logged via email or phone to ensure accountability and tracking.	Inspected a sample of IT support email requests to confirm that user requests are logged, tracked, and addressed appropriately.	No Exceptions Noted
CC7.3	**Security Incidents: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.**			
	Incident Management Policy	The Organization has a formal, documented incident management process defined within its Information Security Policies. The process outlines the evaluation, classification, and handling of reported security and operational events.	Reviewed the Organization's ISMS and Information Security Policies to confirm that a formal incident management process is documented.	No Exceptions Noted
	Incident Tracker	All reported incidents are communicated to the IT team and tracked through an incident management tracker to ensure timely resolution and accountability.	Inspected tracker of the incident management to verify that reported incidents are recorded and tracked.	No Exceptions Noted
	Incident ticket details captured	Reported incidents are logged as tickets within the incident management system. Each ticket includes the following details: Severity of the incident Date and time of occurrence Description of the incident Status of resolution Root cause analysis (for high-severity incidents)	Inspected tracker of the incident management to verify that reported incidents are recorded and tracked.	No Exceptions Noted
CC7.4	**Response to security incidents: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.**			

	Review of incidents in committee meetings	The Organization's management reviews all security and operational incidents periodically. Corrective and preventive actions are identified and tracked to ensure resolution and to mitigate recurrence.	Enquired with management to verify that follow-up actions from incidents are completed in a timely manner.	No Exceptions Noted
	Change Management for repeated incidents	For incidents requiring permanent remediation, the Organization initiates formal change management requests. This ensures that repeated issues are resolved through controlled system or process modifications.	Reviewed the Incident Management Procedure to confirm that change requests are raised for incidents requiring permanent fixes.	No Exceptions Noted
CC7.5	**Recover from Security incidents: The entity identifies, develops, and implements activities to recover from identified security incidents.**			
	RCA for incidents	The Organization performs root cause analysis (RCA) for all major or critical incidents. This process identifies underlying causes to prevent recurrence and to support corrective and preventive actions.	Enquired with IT staff and management to confirm that procedures are in place to perform root cause analysis for major or critical incidents. Noted that no major incidents occurred during the audit period.	No Exceptions Noted
8	**Change Management:**			
CC8.1	**Change Management: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**			
	Change management policy	The Organization has documented change management and approval processes in its Information Security Policies. These processes ensure that changes to systems, applications, and infrastructure are controlled, authorized, and tracked.	Reviewed the Information Security Policies to confirm that change management policies and procedures are defined.	No Exceptions Noted
	SDLC Policy	Software design and development procedures, including change management for development activities, are documented in the Organization's Software Development Life Cycle (SDLC) process.	Inspected SDLC documentation to confirm that software design and development change procedures are formally documented.	No Exceptions Noted

	Development Peer review	All software changes are peer reviewed by another developer to ensure consistency, quality, and adherence to coding standards.	Enquired with management to confirm that informal code review by a peer programmer is performed for all changes.	No Exceptions Noted
	Regression Testing	The testing team prepares system and regression testing using approved test plans and test data to ensure that new changes do not adversely impact existing functionality.	Reviewed test plans for a sample of releases to confirm inclusion of regression and security testing steps.	No Exceptions Noted
	Software code on GIT/SVN	All software code is maintained in a version-controlled repository GitHub to ensure traceability and proper change management.	Inspected screenshot of GitHub to determine that software code is maintained in GitHub	No Exceptions Noted
	QA testing / UAT testing	Software changes undergo unit testing, QA testing, and User Acceptance Testing (UAT). Each activity is documented and monitored through the change request process.	Reviewed a sample of change requests to confirm that QA and UAT testing were performed and documented.	No Exceptions Noted
	Separate environment for changes	Development, testing, and production environments are segregated. Developers do not have direct access to modify testing or production environments, ensuring controlled deployment of changes.	Enquired with management to confirm segregation of development, testing, and production environments and to understand the process for implementing major changes.	No Exceptions Noted
	Rollback plans	All change requests include implementation and rollback (back-out) plans. Code repositories and deployment tools support reverting changes if necessary.	Reviewed a sample of change requests to confirm that rollback plans were included and documented.	No Exceptions Noted
9	**Risk Mitigation:**			
CC9.1	**Risk mitigation: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**			

	BCP Plan and documentation	The Organization has a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) guideline. These documents define the procedures and responsibilities for responding to events that impact systems or infrastructure, ensuring continuity of critical operations.	Reviewed the Organization's BCP and DR policies and procedures to confirm that a formal plan is documented with clear roles and responsibilities for personnel required to respond during a disruption.	No Exceptions Noted
	BCP Testing	The Organization plans to test its Business Continuity and Disaster Recovery procedures, including restoration of backups, on an annual basis to validate their effectiveness.	Reviewed the Business Continuity Planning Policy to confirm that BCP and DR plans are scheduled for annual testing. Reviewed the tabletop exercise document and noted that no BCP testing was performed during the audit period.	No Exceptions Noted
CC9.2	**Risk mitigation: The entity assesses and manages risks associated with vendors and business partners.**			
	Vendor Selection Process	New Third Party Service Providers are selected based on a Vendor Selection Process. Privacy and Security risk assessment is a key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestations such as ISO 27001, SOC1 or SOC2.	Enquired with Management that vendors and third party service providers are selected based on a vendor due diligence. Enquired with Management that there was no material third party vendor that was onboarded during the audit period.	No Exceptions Noted
	Audit reports, SOC reports for Vendors	Company obtains and reviews compliance reports and certificates such as PCI DSS, ISO 27001, SOC1 or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring.	Inspected sample certification and attestation reports of Company's vendors to determine that the company receives such reports that are used in monitoring controls.	No Exceptions Noted

	Contracts with Third Party Processors	A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.	Inspected a sample of Third-Party contracts to determine that Third Party contracts are in place. Enquired with Head Payroll that there are no new Third Party that are onboarded during the current period.	No Exceptions Noted

A	ADDITIONAL CRITERIA FOR AVAILABILITY:			
A1.1	**Processing Capacity Monitoring: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.**			
	Redundancy	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inspected redundancy measures for firewall and determined that there is a backup firewall in a high availability configuration	No Exceptions Noted
A1.2	**Environmental Controls and Backup: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.**			
	Environmental Controls	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared.	Observed that fire extinguisher across all office premises that these are in working condition. Observed other environmental controls.	No Exceptions Noted
	Fire drill	Fire drill is conducted annually.	Observed the fire drill report and verified that there were no exceptions noted.	No Exceptions Noted
	UPS, DG	Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. DG set of sufficient capacity is provided to provide power during outage.	Physically observed the UPS and DG Set installed at the premises to determine that they are in good working condition.	No Exceptions Noted

	Server room temperature	IT Engineer monitors the temperature in server room on a daily basis and take corrective actions in case of discrepancy.	Selected a sample of dates and inspected the server room temperature monitoring records to determine that server room temperatures are monitored.	No Exceptions Noted
	Maintenance Checklist	Facilities and admin personnel monitor the status of environmental protections on a regular basis. Maintenance checklists are used where applicable.	Inspected environmental control check report and determined that maintenance reviews are carried out. Inspected the UPS and DG preventive maintenance reports, vendor maintenance contracts to determine that preventive maintenance is performed periodically.	No Exceptions Noted
A1.3	**Business Continuity: The entity tests recovery plan procedures supporting system recovery to meet its objectives.**			
	BCP DR Plans	Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented.	Inspected disaster recovery & Business Continuity plans to determine that these are documented.	No Exceptions Noted
C	**ADDITIONAL CRITERIA FOR CONFIDENTIALITY:**			
C1.1	**Data Retention: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**			
	Retention policy	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company retains information as per the defined policies.	No Exceptions Noted
C1.2	**Data Deletion: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**			
	Retention policy	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the retention policy to determine that the Company retains information as per the defined policies.	No Exceptions Noted

*** END OF THE REPORT ***