Kaar Technologies India Pvt Ltd & its subsidiaries

Report on KaarTech's Description of its Digital Transformation Services and the Suitability of the Design and Operating Effectiveness of its Controls

System and Organization Controls

SOC 2 Type 2 Report

Throughout the period January 1, 2024, to March 31, 2025

STATEMENT OF CONFIDENTIALITY

This report is intended solely for use by the management of KaarTech, its user entity that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of user entity (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), the use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk.

The unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of KaarTech

Scope

We have examined Kaar Technologies India Pvt Ltd & its subsidiaries (hereinafter called as KaarTech) for its 'Digital Transformation Services' (description), throughout the period January 1, 2024 to March 31, 2025 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report with Revised Implementation Guidance-2022 (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024 to March 31, 2025, to provide reasonable assurance that KaarTech's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria)*.

KaarTech uses AWS Cloud Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at KaarTech, to achieve KaarTech's service commitments and system requirements based on the applicable trust services criteria.

The description presents KaarTech's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of KaarTech's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the KaarTech's controls are suitably designed and operated effectively, along with related controls at the Kaar Technologies. 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.

Service Organization's Responsibilities

In Section 2, KaarTech has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description.

KaarTech is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives, and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description, the suitability of the design, and the effectiveness of the operating controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we 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.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is 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.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements 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.

Service Auditor's Independence and Quality Control
We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement. We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintained a comprehensive system of quality control.

Inherent Limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls 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 conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls
The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4 of this report.

Basis for Qualified Opinion
The accompanying description includes controls that were not in place during the audit period:

- VAPT was not performed during the audit period.
- The user access review for KTern was not performed.
- The firewall ruleset review was not performed during the audit period.
- Network changes were not documented.
- BCP/DR test was not performed during the audit period.

Opinion
In our opinion, except for the possible effects of the matters giving rise to the modification described in the preceding paragraph, in all material respects, based on the criteria described in KaarTech's assertion:

- the description presents 'KaarTech's Digital Transformation Services' was designed and implemented throughout the period January 1, 2024, to March 31, 2025 in accordance with the description criteria

- the controls related to control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2024, to March 31, 2025; and user

entity applied the complementary controls assumed in the design of the KaarTech's controls throughout the period January 1, 2024, to March 31, 2025.

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2024, to March 31, 2025, if complementary user entity controls assumed in the design of KaarTech's controls operated effectively throughout the period January 1, 2024, to March 31, 2025.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of KaarTech, user entities of KaarTech's services during some or all of the period January 1, 2024 to March 31, 2025, business partners of KaarTech subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- 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 service organization's service commitments and system requirements 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.

Truly Yours,

ControlCase Assurance

Yusufali and Associates, LLC dba ControlCase Assurance,

Date : May 23, 2025

SECTION 2 ASSERTION OF KAARTECH'S MANAGEMENT

Kaar Technologies India Pvt Ltd
Level 8, Shyamala Towers,
No. 136, Arcot Road,
Chennai- 600 093, TN, INDIA
CIN: U72200TN2005PTC087065
e | info@kaartech.com
w | www.kaartech.com

KAAR TECHNOLOGIES' ASSERTION

We have prepared the accompanying description of Kaar Technologies India Pvt Ltd & its subsidiaries for its Digital Transformation Services (description) throughout the period January 1, 2024 to March 31, 2025 (description) based on the criteria for a description of the service organization's system in *DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report with Revised Implementation Guidance-2022 (AICPA, Description Criteria), (description criteria).*

The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that Kaar Technologies has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity and Privacy (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria).*

Kaar Technologies uses AWS Cloud Services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kaar Technologies, to achieve Kaar Technologies' service commitments and system requirements based on the applicable trust services criteria. The description presents Kaar Technologies' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Kaar Technologies' controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at Kaar Technologies, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Kaar Technologies' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Kaar Technologies' controls.

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

1) Except for the matter described in paragraph 3, the description fairly presents Kaar Technologies' Digital Transformation Services that was designed and implemented throughout the period throughout the period January 1, 2024 to March 31, 2025, in accordance with the description criteria.

2) Except for the matter described in paragraph 3, the controls stated in the description were suitably designed throughout the period January 1, 2024 to March 31, 2025, to provide reasonable assurance that Kaar Technologies' service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively and user entity applied the complementary controls assumed in the design of Kaar Technologies' controls throughout that period.

3) The description includes controls that were not in place during the audit period:
   - VAPT was not performed during the audit period.
   - The user access review for KTern was not performed.
   - The firewall ruleset review was not performed during the audit period.
   - Network changes were not documented.
   - BCP/DR test was not performed during the audit period.

Yours Truly

Srinivasan Subbiah
Chief Information Officer
Kaar Technologies
Date : May 22, 2025

SECTION 3 DESCRIPTION OF THE KAARTECH'S DIGITAL TRANSFORMATION SERVICES SYSTEM

3.1 COMPANY OVERVIEW

KaarTech is a privately held corporation founded in 2005 to provide Digital Transformation Consulting services to its clients worldwide.

The company has 20 years of experience in IT industry . KaarTech's operations include 15+ entities across the globe. The Digital transformation solution combines SAP solutions, Cloud solutions, AI/ML solutions and Digital solutions, SaaS Products such as KEBS, KTern in the IT platform.

KaarTech is a global leader in technology solutions, empowering businesses to thrive in a digital world through innovation, expertise, and customer excellence. Our mission is to drive transformation and deliver value, enabling organizations to harness the power of technology to achieve their business goals and stay ahead in a rapidly evolving marketplace.

With operations spanning 20+ global locations and headquarters in Chennai, KaarTech has successfully executed over 3200+ projects for 440+ global customers, supported by a talented pool of 3500+ employees. Our strategic focus on ensuring customer excellence has earned us 35+ SAP & Business Awards globally. Additionally, we have been recognized as a Great Place To Work organization for three consecutive years.

With a robust track record of executing over 75 S/4HANA Digital Transformation projects worldwide, we are at the forefront of the digital transformation wave, powered by our IP, KTern.AI. Through its Gen AI approach, this tool enables global enterprises to achieve accelerated and intelligent SAP S/4HANA transformations. Overall, we're committed to transforming enterprises and securing their success in this digital era. For more info, visit - www.kaartech.com

Our Brand Tagline: Dependable Partner, Trustworthy Services!

Our Mission: To remain a socially responsible corporate entity, which will instill a sense of pride, joy and accomplishment, in every facet of its interaction, to everyone associated, be it the employees, customers, vendors or stakeholders.

Our Vision: To be the most Dependable and Trustworthy partner in our customer's Digital Transformation journey by providing Best in Class Products, Services and Execution.

3.2 DESCRIPTION OF SERVICES PROVIDED

KaarTech provides Digital Transformation Services to large employers, and government entities that operate their own IT wings to meet their compliance needs. KaarTech monitors the security and availability of the data center infrastructure and the KaarTech application.

KaarTech provides SAP Solutions and Digital Transformation through proven, agile, and customer-focused frameworks. With an AI-First approach we create intelligent, future proof digital solutions for business that transform the experience of customers, employees and stakeholders. We offer secure, managed cloud solutions that support transformation and outcome-based modernization, driving success through continuous innovation and tailored services for business needs. We also do Data analytics, Business Process Management, Product Engineering etc. We have SaaS products called KEBS, KTern, K4K (KEBS for Kaar).

More information about the KaarTech organization and a description of services can be found at www.kaartech.com .

3.3 SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by the management to customers regarding the performance of KaarTech's services. System requirements are specifications regarding how the system should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company policies and procedures. KaarTech has made commitments to ensure security and fulfill service levels agreements. The Company's principal service commitments and system requirements related to Digital Transformation Services include the following:

Security

KaarTech has made commitments related to security and complying with relevant laws and regulations. These commitments are addressed through relevant logical and physical security controls designed to prevent unauthorized access to the infrastructure and service that support the system and use of encryption technologies.

Service Levels

KaarTech has made commitments to customers with regards to service levels. This involves meeting or exceeding the established SLA, ensuring that the quality of service provided is consistent and reliable and addressing any issues or problems that arise promptly and effectively. In order to ensure that service levels are met, and commitments are fulfilled, KaarTech has implemented processes and procedures that monitor and measure the performance of their services and take corrective action when necessary. KaarTech has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and contracts with customers.

3.4 OVERVIEW OF SYSTEM

The system consists of multiple components such as policies and procedures, Governance Structure, Support Functions, and systems used to provide the services. The policies and procedures guide the users regarding the process to be followed for providing the services and assists in the consistent implementation of the same. The Governance Structure establishes a structure for operating the system and assists in demonstrating management commitment for the same. Internal control consists of the following interrelated components. These are derived from the way management runs a business and are integrated with the management process. KaarTech has established an internal control framework that reflects the COSO framework's five components, described below:

- Control Environment is the foundation to implement internal controls, providing standard requirements and system structure and influencing the employee's internal control awareness.
- Information and Communication ensures that employees obtain and communicate information about internal controls that need to be implemented through an information and communication system and manages the operation of information communication

activities.

- Risk Assessment identifies and systematically analyzes relevant risks which may threaten the achievement of control objectives in operational activities, forming a reasonable strategy to respond to risks.
- Monitoring Activities to monitor the entire internal control procedure and implement remediation when necessary; if conditions permit it, adjust the corresponding control procedures to ensure a timely response of the internal control system.
- Control Activities to establish and implement control policies, procedures, standards, and work instructions to ensure that the controls designed by management are effective to address risks to achieve the entity's control objectives and are designed & operating effectively.

3.5 SYSTEM BOUNDARIES & COMPONENTS OF THE SYSTEM

Based on the criteria set forth in the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality, Processing Integrity, Privacy (SOC 2®) (description criteria), a system is designed to achieve specific business objectives in accordance with management-specified requirements.

This report addresses the following five components of the KaarTech's System, which comprise the boundaries of the system:

- Infrastructure. The physical infrastructure comprises of IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks, Servers, Networks and security tools) and AWS cloud hosted services of KEBS, KTern & K4K (KEBS for Kaar).
- Software. The application programs and IT system software that support application programs (operating systems, middleware, SaaS applications and utilities).
- People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- Processes and Procedures. Automated and manual procedures.
- Data. Transaction streams, files, databases, tables, and output are used or processed by a system.

3.5.1 INFRASTRUCTURE

KEBS

KEBS is hosted in the AWS us-east North Virginia region. VPCs are configured to segregate the network. The application layer, the database layer and the message queuing reside in the private subnet. Whereas the Application load balancer resides in the public subnet. ALB, AWS shield & AWS WAF are deployed to protect the application from the external threats at the perimeter level. NACLs and Security groups are configured to protect the ingress & Egress data traffic.
The microservices based application is hosted in the Docker container under the AWS EC2.
AWS RDS RDS with the MySQL engine configured as a primary Database server and with two read

replicas. To ensure the business continuity and data availability, KEBS systems enabled with cross region back up which data backup in different region with the retention of 30 days and point-in-time-recovery which Enables the restoration of the database to any specific point in time within the retention period. Data are stored EBS Volume which has storage autoscaling and encryption at rest. Static data are stored in the AWS S3 and configured with the bucket policy.
Regular Backups are taken every day with a retention of 30days.To protect the cryptographic keys, AWS KMS configured to secure the data across S3, RDS and EBS.
AWS Cloud Watch configured to provide centralized monitoring for logs, metrics, and alerts across all AWS resources.

KTern

KTern hosted in AWS us-east North Virginia region and deployed as a monolithic architecture, where the entire application is deployed as a single unit on an Ubuntu-based EC2 instance and containerized in AWS ECS in single availability zone. The application is hosted on a private subnet with the VPCs and security groups configured to segregate and protect the network traffic. For data storage, KTern uses MongoDB Atlas, a cloud-based NoSQL database, and Redis is used as a caching layer to improve performance. Additionally, the DNS management for the application is handled through Google Cloud Platform (GCP). CDN with WAF are enabled to protect the web application from external threats.

Network Zones

The architecture and infrastructure of the KaarTech network is designed and maintained in such a way as to ensure that security and availability are being sustained. The storage, processing, and retrieval of client data and KaarTech corporate data are segregated into different zones. The network architecture of the KaarTech is designed and deployed to ensure the security, availability, integrity, confidentiality and privacy are sustained. Networks are layered into Perimeter, internal sensitive systems, user's networks and segregated with segmentation controls.

Internet border

Next generation firewalls have been configured along with various detection and defense controls.

DMZ

Demilitarized Zone enabled and public facing systems and applications are configured as applicable to protect the sensitive data from internal systems.

Firewall

KaarTech has deployed Palo Alto next generation firewalls with advanced threat management capability to detect and protect its systems and networks from malicious threats.

Production

Servers and networking to support the KaarTech system.Production Business applications and products such as KEBS, KTern are configured as containerized microservices and hosted at AWS cloud. VPCs are configured to segregate the workloads of Production and test environment.

3.5.2 SOFTWARE

KaarTech's products are web-based Software as a Service (SaaS) developed and maintained by its internal software engineering group. The application is built on the following stack:

- Frontend - Angular, Nextjs
- Mobile Frontend - Flutter(Dart)
- Backend - Node.js, Python
- Database - Mongo, Redis,MySQL
- File Storage - S3
- Cloud – AWS
- Project Management - Azure DevOps, JIRA

The application supports all major browsers, including Internet Explorer, Edge, Chrome, Firefox, Safari, and Opera, as well as other up-to-date browsers.

KEBS:

KEBS is a comprehensive PSA platform designed to streamline and automate end-to-end business processes, from initial opportunity management to collections, while integrating seamlessly with third-party applications. Acting as a single source of truth, KEBS prevents revenue leakages and provides a clear, detailed view of budgets and planned vs. actuals at every stage, from quotations to invoicing. Core features include Deal Management with a Quotation Builder for margin planning, Project Planning for defining and monitoring detailed project goals and timelines, and Billing Plan Management with flexible milestone types. People's Allocation capabilities use AI-driven suggestions to ensure optimal resource deployment, while the integrated ATS supports job posting and hiring through to onboarding. Additional features include Timesheet Management for efficient time tracking and payroll integration, Invoicing with seamless billing, payment tracking and monitoring, and a centralized Employee Directory covering the full hire-to-retire cycle. Other modules span Expense and Leave Management, Procure to Pay, Performance Management System, Learning Management System, Visa and Travel, AMS Tickets, Support Tickets, Custom LCDP applications, and forms. With extensive reporting dashboards covering sales performance, project utilization, billing, and financial forecasts, KEBS empowers businesses to maintain compliance, improve decision-making, and maximize operational efficiency.

KTern:

KTern.AI is an SAP Spotlight Partner with the vision to inspire and democratize SAP centric Digital Transformation as Service (DXaaS). With DXaas as platform KTern.AI ensure success. KTern is used to extensively study an existing SAP system and determine the functional, technical and business impact of an SAP Digital Transformation.

Digital Maps is used to study the existing SAP system and determine functional, technical and business impact of SAP digital transformation.

Digital Projects are used to gain ultimate control of the SAP digital transformation through a unified cognitive digital workplace which promotes real time collaboration, rigid governance, and automated signoffs.

Digital Process is used to achieve business process control and visibility which enables integrity between business processes and project tasks

Digital Labs is used to automate all aspects of SAP Testing, Test preparation, Test Execution, Test documentation, Test monitoring, Test Sign off and Test management.

Digital mines is used to mine existing business processes, identify areas of optimization, and analyze the impact of change on process and test during each release.

3.5.3 PEOPLE

To meet its commitments and requirements, KaarTech has defined organisational structures, reporting lines, authorities, and responsibilities for the system's design, development, implementation, operation, maintenance, and monitoring.

3.5.4 POLICIES & PROCEDURES

KaarTech maintains documented policies and procedures to guide personnel in carrying out their responsibilities, classifying system alerts, documenting incidents, monitoring performance etc. Regular reporting is utilized by management to identify deviations from documented policies and procedures and guide corrective actions. All relevant policies are reviewed at least annually or when significant changes occur to ensure their continuing adequacy and effectiveness.

3.5.5 DATA

KaarTech applications [KEBS, KTern] are hosted on AWS, with each customer restricted to viewing data within their dedicated database. Customers are responsible for managing user access permissions for authorized personnel. Data is entered into the system through manual input, device integrations, or electronic file uploads. Before being accepted, all input data undergoes validation to ensure compliance with predefined business rules, syntax, and semantic integrity, including character set validation, length constraints, numerical range enforcement, and acceptable value checks. The system ensures that all inputs conform to specified format and content requirements, maintaining audit logs for traceability.

3.6 RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, MONITORING ACTIVITIES, AND CONTROL ACTIVITIES

3.6.1 CONTROL ENVIRONMENT

KaarTech’s control environment reflects the leadership team's commitments on the importance of controls and the emphasis is given through its policies and procedures.

KaarTech's control environment reflects the overall attitude, awareness, and actions of management and employees concerning the importance of controls and their emphasis within KaarTech.

Integrity and ethical values are essential components of the control of the environment, affecting the design, administration, and monitoring of the solution. KaarTech communicates organizational integrity and values through the actions of executive leadership, documented policies. The policies and procedures are communicated to employees and are available via K4K system and Teams channel.

3.6.2 RISK ASSESSMENT

KaarTech regularly reviews the risks that may threaten the achievement of the criteria for the security principle. The leadership team assesses security risks on an ongoing basis. This is done through regular management meetings, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment. The risk management program encompasses the following phases:

- Identify – These efforts identify technical and business risks to the organization and operations.
- Assess – The assessment phase evaluates the potential impact(s) of identified risks, the likelihood of occurrence, and control effectiveness and maturity.
- Mitigate – Mitigation develops risk treatment plans to control or reduce risk where needed, including the implementation of controls, processes, and other physical and virtual safeguards.
- Report – Reporting and communication are performed to ensure that risk owners and stakeholders, as well as senior leadership, have visibility into risks to the organization and that there is effective decision-making around risks.
- Monitor – Identified and assessed risks are periodically reviewed, along with any associated risk response efforts for the risk, to determine if their state or status has changed.

The strategic plan for its technology is developed by the leadership team.

KaarTech maintains insurance policies to manage and mitigate potential losses and risks.

3.6.3 INFORMATION AND COMMUNICATION

KaarTech management uses various and tailored methods to communicate with employees. A few of the key reasons to communicate include sharing company and industry news, contacting all employees in the event of a significant event, and ensuring employees understand company policies, standards, and procedures. Examples of communication methods include Townhall sessions, new hire orientation and training, video conferencing, email, internal chat, all-employee meetings, project team meetings, department meetings, etc.

Every employee needs to sign an NDA as part of the employee agreement, which formally defines all the rules and regulations required to follow during employment.

Customer and vendor contracts and nondisclosure agreements (NDAs) explicitly address KaarTech's security, Availability, Confidentiality, Privacy, Processing Integrity commitments and the associated system requirements. Additionally, client agreements and statements of work clearly

define KaarTech's system boundaries, responsibilities, and service expectations, which are provided to customers during the onboarding process.

3.6.4 MONITORING ACTIVITIES

Management has established monitoring processes to provide appropriate oversight, assess ongoing vulnerabilities, and identify and respond to incidents.

3.6.5 CONTROL ACTIVITIES

Logical Security

- The following logical access controls have been implemented:
- Management has established policies and procedures pertaining to user account management.
- User access is restricted on a "need to know" basis using the principle of least privilege.
- Unique user IDs are assigned to individual users.
- Authentication to the network and applications requires a unique user ID and strong password.
- Authentication for access to client data requires a business need, management approval, and two-factor authentication consisting of login credentials and a hardware authentication device that supports one-time passwords.

Physical Security

Physical access to KaarTech premises is controlled through electronic proximity cards, video surveillance, round the clock security guards deployed at the main entrance and building premises to monitor the movement of people and equipment in and out of the premises.
Internal process guidelines for access control and ID Card management are developed for the issuance of photo ID cards, activation, deactivation, and reconciliation of access records. Close-circuit television (CCTV) cameras are installed at suitable locations within the premises.
Physical access to corporate premises is set up for authorized new joiners based as part of the onboarding process. Physical access is revoked from the access control system as a part of the employee separation process. Processes are in place to recover entity devices.

Environmental protections are installed which includes the following:

- Cooling systems
- Fire Suppression system
- UPS System

KaarTech has contracts with third-party vendors for maintenance of the air-conditioning units, monitoring of the fire alarms, activation of the sprinkler system, and fire extinguishers, and emergency lighting.

Security administration

- User Access Management: User access to the applications is provisioned based on role-based access control (RBAC), ensuring employees and contractors are granted permissions aligned with their job responsibilities.
- User Deprovisioning & Access Reviews: Employee terminations are promptly communicated, ensuring that the applications access is revoked immediately upon termination.

Authentication mechanism
Authentication and access to the applications are managed through Single Sign-On (SSO). These solutions enforce strong authentication policies, including multi-factor authentication (MFA), to ensure secure and seamless access to cloud resources while maintaining compliance with security best practices.

Network security
The details of the Company's information systems are documented via network diagrams, and these are available to authorized users. The security and health of the network is monitored using network monitoring tools.

Incident management
KaarTech has documented Incident Management Procedure to ensure that information security events and weaknesses are promptly reported to allow timely corrective actions to be taken.

Data encryption
KaarTech supports 256-bit asymmetric cryptographic encryption (TLS) to secure communication. Data is signed using a secure certificate from a trusted certificate authority, and user authentication is enforced through valid session credentials, including a username/password combination.

Virus protection
KaarTech uses McAfee AV solution.

Change management
KaarTech has established a structured Change Management process to ensure segregation of duties and maintain the integrity, security, and stability of the environment. The process ensures that authorization, development, testing, and implementation are distinct functions, minimizing risk and enforcing compliance.

Patch management
KaarTech has implemented patch management process to guide personnel in the initiation, testing, and deployment of patches for production infrastructure. This ensures timely updates to address security vulnerabilities and performance improvements while minimizing operational disruptions.

Confidentiality & Data Privacy
KaarTech has established a comprehensive set of policies and procedures to ensure the confidentiality, integrity, and security of client-sensitive information. These policies align with industry best practices and regulatory requirements to safeguard data throughout its lifecycle. KaarTech's Code of Conduct mandates that all employees and contractors adhere to the highest standards of confidentiality when handling customer information. All personnel must restrict access to sensitive information strictly to those with a business need to know and comply with company proprietary data protection policies.

Vendor management
Agreements are established with third-party vendors and service providers relevant to the system, including clearly defined terms, conditions, and responsibilities. Responsibilities include confidentiality and privacy commitments as applicable.

3.7 COMPLEMENTARY USER ENTITY CONTROLS

KaarTech's services are designed assuming user entities implement certain controls. Such controls

are called complementary user entity controls. It is not feasible for all the Trust Services Principles related to KaarTech's services to be solely achieved by KaarTech's control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Kaar Technologies.

User entities should implement complementary user entity controls to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

User Entity Control	Associated Criterion
User entities are responsible for understanding and complying with their contractual obligations to Kaar Technologies.	CC2.3
User entities are responsible for immediately notifying KaarTech of any actual or suspected information security breaches or violations of confidentiality agreements.	CC7.2
User entities are responsible for notifying KaarTech of any regulatory issues that may affect the company's services.	CC7.2 CC7.3 CC7.4 CC9.2
User entities are responsible for establishing procedures for developing, maintaining, and testing their business recovery/continuity plans separate from Kaar Technologies.	A1.2 A1.3
User entities are responsible for immediately notifying KaarTech of any changes to existing confidentiality agreements that could affect the integrity of sensitive data.	CC2.3 CC9.2 CC1.1
User entities are responsible for establishing controls to restrict access to the platform to authorized personnel only, including deactivation of customer user accounts for terminated personnel.	CC6.1 CC6.2 CC6.3
User entities are responsible for ensuring procedures are in place for periodic user access review to confirm that access to the platform is appropriate.	CC5.1 CC6.2
User entities are responsible for notifying KaarTech of changes made to technical or administrative contact information.	CC2.3

3.8 SUBSERVICE ORGANIZATION

KaarTech leverages AWS cloud infrastructure for hosting its applications. Although the subservice organization has been "carved out" for this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. It is expected that Cloud Service Providers will implement the following types of controls specified below to support the achievement of the associated criteria. The list below should not be regarded as a comprehensive list of all controls that subservice organizations should employ.

Complementary Subservice Organization Controls	Associated Criterion
Subservice providers are responsible for managing logical access to underlying infrastructure components for cloud service.	CC6.1 CC6.2

	CC6.5
Subservice providers are responsible for managing physical security controls for data center facilities.	CC6.4 CC6.5
Subservice providers are responsible for decommissioning and securely erasing production media prior to removal from the cloud hosting environment.	CC6.5
Subservice providers are responsible for movement and removal of physical storage devices in the cloud hosting environment.	CC6.7
Subservice providers are responsible for monitoring for anomalies which are indicative of natural disasters having the potential to affect hosting facilities.	CC7.2
Subservice providers are responsible for maintaining the availability of the cloud hosting environment.	CC7.2
Subservice providers are responsible for identifying environmental threats, designing detection measures, monitoring, responding and communicating these to Kaar Technologies.	A1.2

3.9 DISCLOSURE OF SYSTEM INCIDENTS

There were no incidents that are likely to affect report users' understanding of how KaarTech is used to provide the services through the period from January 1, 2024 to March 31, 2025.

3.10 DISCLOSURE OF SIGNIFICANT SYSTEM CHANGES

There were no changes that are likely to affect report users' understanding of how the KaarTech is used to provide services through the period from January 1, 2024, to March 31, 2025.

3.11 APPLICABLE TRUST SERVICES CRITERIA

Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives. Security refers to the protection of

- information during its collection or creation, use, processing, transmission, and storage and
- systems that use electronic information to process, transmit or transfer and store information to enable the entity to meet its objectives.

Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability. Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality. Information designated as confidential is protected to meet the entity's objectives. Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries).
Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel.
Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

Privacy. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Although confidentiality applies to several types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized as follows:

- Notice and communicate objectives. The entity provides notice to data subjects about its objectives related to privacy.
- Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
- Collection. The entity collects personal information to meet its objectives related to privacy.
- Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
- Access. The entity provides data subjects with access to their personal information

for review and correction (including updates) to meet its objectives related to privacy.

- Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
- Quality. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
- Monitoring and Enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Relevant trust services criteria and related controls are included in Section 4 of this report, "Trust Services Criteria, KaarTech Related Controls, Independent Service Auditor's Description of Tests of Controls and Results". Although the applicable trust services criteria and related controls are presented in Section 4, they are, nevertheless, an integral part of KaarTech description.

SECTION 4 DESCRIPTION OF KAARTECH'S CONTROL OBJECTIVES, RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

4.1 INFORMATION PROVIDED BY INDEPENDENT SERVICE AUDITOR EXCEPT FOR TRUST SERVICES CRITERIA AND RELATED CONTROLS

INTRODUCTION

This report, including the description of tests of controls and results thereof in this section, is intended solely for the information and use of Kaar Technologies, user entity of the Digital Transformation Services during some or all of the period January 1, 2024 to March 31, 2025, business partners of KaarTech subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, and other parties.
- Complementary user entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- Internal Control and its limitations.
- Description criteria.
- And the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This section presents the following information provided by Kaar Technologies.

- Column 1: Relevant Trust Services Criteria
- Column 2: Description of KaarTech’s Controls
- Column 3: Service Auditor's Tests of Controls
- Column 4: Results of Service Auditor's Tests of Controls

Our examination was limited to the controls identified by KaarTech to meet the applicable trust services criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy. Our examination did not extend to controls in effect at user entity. It is each interested party’s responsibility to evaluate this information in relation to the controls in place at user organization to assess the total system of internal control.

DESCRIPTION OF TESTING PROCEDURES PERFORMED

Our tests were designed to examine the description of the system as well as the suitability of the design and operating effectiveness of controls for a representative number of samples throughout the period from January 1, 2024, to March 31, 2025.

In addition to the tests listed below, ascertained through multiple inquiries with the management and the control owner, that each control activity listed below operated as described throughout the period.

Tests performed are described below:

Test Approach	Description
Inquiry	Inquiry of the appropriate personnel with the requisite knowledge

	and experience regarding the performance and application of the related control activity.
Observation	Observation of the application, performance, or existence of control during fieldwork.
Inspection	Inspection of documents and reports indicating performance of the control.

4.2 TESTS OF CONTROLS

4.2.1 CC1.0 CONTROL ENVIRONMENT

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	KaarTech has an organizational chart and job responsibilities that identify reporting lines and indicate management levels within the hierarchy.	Inspected the organizational chart from the company to determine whether functional areas, reporting structures within the functional areas, and reporting hierarchies were defined.	No exceptions noted.
CC1.1.2	Personnel must pass a background check as part of the hiring process.	Inspected for the sample new hires that the background checks was completed as part of the hiring process.	No exceptions noted.
CC1.1.3	KaarTech has an Employee Handbook, which is reviewed, updated if applicable, and approved by Senior Management.	Inspected the Employee Handbook to determine whether guidance on employee ethics and the code of business conduct was documented and reviewed by management.	No exceptions noted.
CC1.1.4	KaarTech has identified, documented, and implemented Information Security policy.	Inspected the Information Security and Privacy Policy to determine whether it was in place and was reviewed periodically.	No exceptions noted.
CC1.1.5	Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards.	Inspected the Employee Handbook to determine that a disciplinary process was in place. The process includes the actions taken for employees who violate KaarTech Standards.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	KaarTech has an organizational chart and job responsibilities that identify reporting lines and indicate management levels within the hierarchy.	Inspected that the organizational chart was in place which described the functional areas, reporting structures, etc.	No exceptions noted.

CC1.2.2	Senior Management is responsible and accountable for developing and maintaining the Information Security Program and making policy changes and updates.	Inspected the Information Security and Privacy Policy to determine whether it was in place and that Senior Management is responsible and accountable for developing and maintaining the Information Security Program and policy changes and updates.	No exceptions noted.
CC1.2.3	KaarTech Senior Management and the board of directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and its ongoing risk assessment and management process and revise these when necessary to support achieving objectives.	Inspected the meeting notes of the management meeting to determine whether leadership meetings are held and involve the senior management. Inspected the meeting notes of the management meeting to determine whether Senior Management is responsible for the business planning and the ongoing risk assessment process.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	KaarTech has an organizational chart and job responsibilities that identify reporting lines and indicate management levels within the hierarchy.	Inspected that the organizational chart was in place which described the functional areas, reporting structures, etc.	No exceptions noted.
CC1.3.2	Job descriptions document job requirements, specifying the responsibilities and skills needed.	Inspected the job descriptions for the sample roles to determine whether they were in place and defined the skills, responsibilities, and knowledge levels required for jobs.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Job descriptions document job requirements, specifying the responsibilities and skills needed.	Inspected the job descriptions for the sample roles to determine whether they were in place and defined the skills, responsibilities, and knowledge levels required for jobs.	No exceptions noted.

CC1.4.2	The company provides Security Awareness training upon hire to support the achievement of objectives.	Inspected the security awareness training records for the sample employees to determine whether employees were provided.	No exceptions noted.
CC1.4.3	Personnel must pass a background check as part of the hiring process.	Inspected for the sample new hires that the background checks was completed as part of the hiring process.	No exception noted.
CC1.4.4	Policies and procedures have been prepared and are available to employees.	Inspected that the policies and procedures were in place and were reviewed, updated as needed. Checked that the policy documents were communicated as part of Teams channel announcements.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Job descriptions document job requirements, specifying the responsibilities and skills needed.	Inspected the job descriptions for the sample roles to determine whether they were in place and defined the skills, responsibilities, and knowledge levels required for jobs.	No exceptions noted.
CC1.5.2	Senior Management performs annual performance evaluations to communicate and hold individuals accountable for the performance of internal control responsibilities.	Inspected the internal control matrix and roles and responsibilities defined for key roles and ascertained that performance of the internal controls implemented within the environment were assigned to appropriate departments based on roles and responsibilities.	No exceptions noted.
CC1.5.3	Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards.	Inspected the Employee Handbook to determine that a disciplinary process was in place. The process includes the actions taken for employees who violate KaarTech Standards.	No exceptions noted.

4.2.2 CC2.0 INFORMATION AND COMMUNICATION

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			

CC2.1.1	Data Flow diagram that illustrates the storage, processing, and transmission of the relevant information are documented and maintained by the management.	Inspected the data flow diagram to determine that it illustrated the storage, processing, and transmission of the relevant information documented and maintained by management.	No exceptions noted.
CC2.1.2	Internal audits are conducted, and results are reported to the management. Internal audit findings are analyzed and tracked to closure by implementing the corrective action plan.	Inspected the internal audit report to determine whether internal audits were conducted and whether the results were reported to management.	No exceptions noted.
CC2.1.3	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company provides Security Awareness training upon hire to support the achievement of objectives.	Inspected the security awareness training records for the sample employees to determine whether employees were provided.	No exceptions noted.
CC2.2.2	KaarTech has incident response policies and procedures that include an escalation plan based on the nature and severity of the incident to Senior Management, as necessary.	Inspected the Incident Management Procedure, which is in place and reviewed periodically. Checked that the same include an escalation plan based on the nature and severity of the incident.	No exceptions noted.
CC2.2.3	Policies and procedures are in place to protect these applications and the corresponding client data, as well as logical security, physical security, and environmental controls.	Inspected the Information Security Policy and related policies to determine whether policies and procedures were in place and whether the policies were updated if needed.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			

CC2.3.1	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected the sample agreements with the business partners and service providers to determine whether they included defined terms, conditions, and responsibilities of each party.	No exceptions noted.
CC2.3.2	Documented escalation procedures are in place to guide the third parties in reporting, acting upon, and resolving reported events.	Inspected the company portal to determine whether the contact details (email ID) are made available to report events or maintain open communication.	No exceptions noted.

4.2.3 CC3.0 RISK ASSESSMENT

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to business objectives, commitments and requirements, risk measurement, and response strategy.	No exceptions noted.

CC3.1.2	Management meetings are held to oversee the results of the offered services' operation and anticipate any upcoming risk scenario.	Inspected meeting records to determine that the regular IT meetings and Management meetings are held to oversee operation performance and anticipate any risk scenario.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to business objectives, commitments and requirements, risk measurement, and response strategy.	No exceptions noted.
CC3.2.2	Management performs a fraud risk assessment annually.	Obtained and Inspected KaarTech Risk Assessment & Treatment register to determine whether fraud risks were assessed periodically.	No exceptions noted.
CC3.2.3	KaarTech has identified, documented, and implemented Information Security policy.	Inspected the Information Security and Privacy Policy to determine whether it was in place and was reviewed periodically.	No exceptions noted.
CC3.2.4	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to achieving objectives.			

CC3.3.1	Management performs a fraud risk assessment annually.	Obtained and Inspected KaarTech Risk Assessment & Treatment register to determine whether fraud risks were assessed periodically.	No exceptions noted.
CC3.3.2	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to business objectives, commitments and requirements, risk measurement, and response strategy.	No exceptions noted.
CC3.3.3	Management meetings are held to oversee the results of the offered services' operation and anticipate any upcoming risk scenario.	Inspected meeting records to determine that the regular IT meetings and Management meetings are held to oversee operation performance and anticipate any risk scenario.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the internal control system.			
CC3.4.1	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC3.4 .2	KaarTech Senior Management evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and ongoing risk assessment and management process.	Inspected the meeting notes of the management meeting to determine whether leadership meetings are held and involve the senior management. Verified that the senior management is responsible for the business planning and the ongoing risk assessment process.	No exceptions noted.

	It revises these when necessary to support the achievement of objectives.		
CC3.4.3	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to business objectives, commitments and requirements, risk measurement, and response strategy.	No exceptions noted.

4.2.4 CC4.0 MONITORING ACTIVITIES

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC4.1 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.			
CC4.1.1	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC4.1.2	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.

CC4.1.3	Management obtains and reviews the SOC service auditors' reports from service providers to ensure controls are operating effectively and any identified risks are addressed with the service providers promptly.	Checked that the SOC reports/third-party audit reports are obtained from the critical service provider, which were reviewed.	No exceptions noted.
CC4.1.4	Internal audits are conducted, and results are reported to the management. Internal audit findings are analyzed and tracked to closure by implementing the corrective action plan.	Inspected the internal audit report to determine whether internal audits were conducted and whether the results were reported to management.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	KaarTech has incident response policies and procedures that include an escalation plan based on the nature and severity of the incident to Senior Management, as necessary.	Inspected the Incident Management Procedure, which is in place and reviewed periodically. Checked that the same include an escalation plan based on the nature and severity of the incident.	No exceptions noted.
CC4.2.2	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.

4.2.5 CC5.0 CONTROL ACTIVITIES

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC5.1 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.			
CC5.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to	No exceptions noted.

	risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	business objectives, commitments and requirements, risk measurement, and response strategy.	
CC5.1.2	KaarTech has identified, documented, and implemented Information Security policy.	Inspected the Information Security and Privacy Policy to determine whether it was in place and was reviewed periodically.	No exceptions noted.
CC5.1.3	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC5.1.4	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	KaarTech has identified, documented, and implemented Information Security policy.	Inspected the Information Security and Privacy Policy to determine whether it was in place and was reviewed periodically.	No exceptions noted.
CC5.2.2	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to	No exceptions noted.

	risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	business objectives, commitments and requirements, risk measurement, and response strategy.	
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Policies and procedures are in place to protect applications and the corresponding client data, logical security, etc.	Inspected the Information Security Policy and related policies to determine whether policies and procedures are in place to protect applications and the corresponding client data and whether an annual review was performed, and whether the policies were updated if needed.	No exceptions noted.
CC5.3.2	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected the sample agreements with the business partners and service providers to determine whether they included defined terms, conditions, and responsibilities of each party.	No exceptions noted.

4.2.6 CC6.0 LOGICAL AND PHYSICAL ACCESS CONTROLS

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC6.1 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.			
CC6.1.1	Access control procedures are utilized to grant access to the network and applications; access is granted based on the users' job responsibilities. The user access requests are documented and require approval.	Inspected the Information Security, Access Control policies to determine whether they establish a formal process to grant and deny access to the system components. Inspected for the sample new user onboarding cases that the HR communication for granting the access request was in place.	No exceptions noted.
CC6.1.2	User access reviews are performed periodically to ensure that access to data is restricted.	Inspected the periodic user access review to determine whether it was performed to verify that access to data is restricted to authorized users. It was confirmed that the user access review for KTern was not performed.	The user access review for KTern was not performed.
CC6.1.3	Access is revoked for employees as a component of the employee termination process.	Checked for the sample exited employees that the access revocation was made as per the termination process.	No exceptions noted.
CC6.1.4	The systems are configured to authenticate users and enforce predefined user accounts and minimum password requirements.	Checked that SSO Integration was in place for KEBS, Ktern. Inspected the password configuration at AD level to determine if the password parameters were in accordance with the policy requirements.	No exceptions noted.
CC6.1.5	Remote access for users is facilitated through the GlobalProtect VPN solution. To further enhance security, Multi-Factor Authentication (MFA) has been implemented, adding a layer of protection	Inspected the screenshot of VPN configuration and user list to determine that remote access for users is facilitated through GlobalProtect VPN Solution. Verified that Multi-Factor Authentication was implemented.	No exceptions noted.

	to ensure only authorized users are granted access to the system.		
CC6.1.6	Data Flow diagrams, narratives, and procedures that illustrate the storage, processing, and transmission of the relevant information are documented and maintained by the management.	Inspected the data flow diagrams, narratives, and procedures to determine that it illustrated the storage, processing, and transmission of the relevant information are documented and maintained by the management.	No exceptions noted.
CC6.2 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.			
CC6.2.1	Access control procedures are utilized to grant access to the network and applications; access is granted based on the users' job responsibilities. The user access requests are documented and require approval.	Inspected the Information Security, Access Control, and Physical Access policies to determine whether they establish a formal process to grant and deny access to the system components. Inspected for the sample new user onboarding cases that the HR communication for granting the access request was in place.	No exceptions noted.
CC6.2.2	Access is revoked for employees as a component of the employee termination process.	Checked for the sample exited employees that the access revocation was made as per the termination process.	No exceptions noted.
CC6.2.3	User access reviews are performed periodically to ensure that access to data is restricted.	Inspected the periodic user access review to determine whether it was performed to verify that access to data is restricted to authorized users. It was confirmed that the user access review for KTern was not performed.	The user access review for KTern was not performed.
CC6.3 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.			

CC6.3.1	Access control procedures are utilized to grant access to the network and applications; access is granted based on the users' job responsibilities. The user access requests are documented and require approval.	Inspected the Information Security, Access Control, and Physical Access policies to determine whether they establish a formal process to grant and deny access to the system components. Inspected for the sample new user onboarding cases that the HR communication for granting the access request was in place.	No exceptions noted.
CC6.3.2	User access reviews are performed periodically to ensure that access to data is restricted.	Inspected the periodic user access review to determine whether it was performed to verify that access to data is restricted to authorized users. It was confirmed that the user access review for KTern was not performed.	The user access review for KTern was not performed.
CC6.3.4	Access is revoked for employees as a component of the employee termination process.	Checked for the sample exited employees that the access revocation was made as per the termination process.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	KaarTech facilities are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • Uninterruptible power supply (UPS) systems • Air conditioning units Management retains the inspection report received from third-party specialists, periodically evidencing the completion of inspection and maintenance.	Obtained the inspection reports of air conditioning units, fire detection and suppression equipment, UPS for a sample company facility. Noted that third-party specialists performed the inspections.	No exceptions noted.

CC6.4.2	Close Circuit Television (CCTV) cameras are installed at suitable locations within the premises. Recordings of CCTV logs are available.	Inspected the video feed on the monitor for a selection of days to ascertain whether CCTV recordings were available.	No exceptions noted.
CC6.4.3	Physical access review is performed periodically and required changes are tracked to completion.	Inspected the sample of physical access review report to determine whether physical access review was performed periodically.	No exceptions noted.
CC6.5 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.			
CC6.5.1	Policies and procedures are in place to guide personnel in data, hardware, and software disposal and destruction. Data that is no longer required for business purposes is rendered unreadable.	Inspected Kaar Tech - Scrap Policy to determine that policies and procedures are in place to guide personnel in data, hardware, and software disposal and destruction. Inquired about the data disposal process to determine that data no longer required for business purposes is rendered unreadable. The service auditor was informed that no media or hardware disposal occurred during the audit period.	No exceptions noted.
CC6.5.2	Access is revoked for employees as a component of the employee termination process.	Checked for the sample exited employees that the access revocation was made as per the termination process.	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	PA firewall with IPS modules are implemented to prevent intrusions into the network.	Inspected the network diagram and firewall ruleset to ascertain whether PA firewall with IPS modules was implemented to prevent the network from unauthorized access.	The firewall ruleset review was not performed during the audit period.

		It was confirmed that the firewall ruleset review was not performed during the audit period.	
CC6.6.2	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
CC6.6.3	FIM solution is implemented to monitor and detect unauthorized changes to system files.	It was confirmed that no FIM solution was in place.	No FIM solution was in place.
CC6.6.4	Network and system software patches and updates are applied to the security systems as needed.	Inquired of Management to determine whether the IT team is responsible for patch management. Inspected evidence of patch updates to determine whether the patches were applied.	No exceptions noted.
CC6.6.6	End-User does not have permission to install software on the workstations. The ability to install software is restricted to authorized administrators.	Verified that the ability to install software is restricted to authorized administrators.	No exceptions noted.
CC6.6.7	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations.	Checked that Mcafee AV was in use for servers, endpoints.	No exceptions noted.
CC6.6.8	The usage of removable media was restricted using DLP.	Checked that the usage of removable media was restricted using McAfee DLP module.	No exceptions noted.
CC6.6.9	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.
CC6.7 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.			

CC6.7.1	End-User does not have permission to install software on the workstations. The ability to install software is restricted to authorized administrators.	Verified that the ability to install software is restricted to authorized administrators.	No exceptions noted.
CC6.7.2	The usage of removable media was restricted using DLP.	Checked that the usage of removable media was restricted using McAfee DLP module..	No exceptions noted.
CC6.7.3	Encryption technologies are used to protect data at rest and in transit.	Inquired of management and confirmed that data at rest and in transit is encrypted using strong encryption technologies. Inspected the encryption configuration and ascertained that data at rest is encrypted using AES 256 and VPN Tunnels, SSL/TLS, is used for data in transit.	No exceptions noted.
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations.	Checked that Mcafee AV was in use for servers, endpoints.	No exceptions noted.
CC6.8.2	End-User does not have permission to install software on the workstations. The ability to install software is restricted to authorized administrators.	Verified that the ability to install software is restricted to authorized administrators.	No exceptions noted.
CC6.8.3	FIM solution is implemented to monitor and detect unauthorized changes to system files.	It was confirmed that no FIM solution was in place.	No FIM solution was in place.

4.2.7 CC7.0 SYSTEM OPERATIONS

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC7.1 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.			
CC7.1.1	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations.	Checked that Mcafee AV was in use for servers, endpoints.	No exceptions noted.
CC7.1.2	PA firewalls with IPS modules are implemented to prevent intrusions into the network.	Inspected the network diagram and firewall ruleset to ascertain whether PA firewall with IPS modules was implemented to prevent the network from unauthorized access. It was confirmed that the firewall ruleset review was not performed during the audit period.	The firewall ruleset review was not performed during the audit period.
CC7.1.3	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
CC7.1.4	FIM solution is implemented to monitor and detect unauthorized changes to system files.	It was confirmed that no FIM solution was in place.	No FIM solution was in place.
CC7.1.5	Vulnerability assessments and penetration testing are performed periodically.	It was confirmed that VAPT was not performed during the audit period.	VAPT was not performed during the audit period.

CC7.2 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 analyzed to determine whether they represent security events.			
CC7.2.1	PA firewall with IPS modules are implemented to prevent intrusions into the network.	Inspected the network diagram and firewall ruleset to ascertain whether PA firewall with IPS modules was implemented to prevent the network from unauthorized access. It was confirmed that the firewall ruleset review was not performed during the audit period.	The firewall ruleset review was not performed during the audit period.
CC7.2.2	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
CC7.2.3	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations.	Checked that Mcafee AV was in use for servers, endpoints.	No exceptions noted.
CC7.2.4	Vulnerability assessments and penetration testing are performed periodically.	Inspected the vulnerability assessments and network penetration test reports to determine whether they were performed during the audit period.	No exceptions noted.
CC7.3 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.			
CC7.3.1	KaarTech has documented Information Security Incident Management Procedure to ensure that information security events and weaknesses are promptly reported to allow timely corrective actions to be taken.	Inspected the Incident Management Procedure, which is in place and reviewed periodically. Checked that the same include an escalation plan based on the nature and severity of the incident.	No exceptions noted.

CC7.3.2	Reported incidents are logged & resolved as per Incident Managent policy requirement.	Checked that there was only one incident raised during the audit period which was logged & resolved.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents as appropriate.			
CC7.4.1	KaarTech has documented Information Security Incident Management Procedure to ensure that information security events and weaknesses are promptly reported to allow timely corrective actions to be taken.	Inspected the Incident Management Procedure, which is in place and reviewed periodically. Checked that the same include an escalation plan based on the nature and severity of the incident.	No exceptions noted.
CC7.4.2	Reported incidents are logged & resolved as per Incident Management policy requirement.	Checked that there was only one incident raised during the audit period which was logged & resolved.	No exceptions noted.
CC7.4.3	Network and system software patches and updates are applied to the security systems as needed.	Inquired of Management to determine whether the IT team is responsible for patch management. Inspected evidence of patch updates to determine whether the patches were applied.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	KaarTech has documented Information Security Incident Management Procedure to ensure that information security events and weaknesses are promptly reported to allow timely corrective actions to be taken.	Inspected the Incident Management Procedure, which is in place and reviewed periodically. Checked that the same include an escalation plan based on the nature and severity of the incident.	No exceptions noted.

4.2.8 CC8.0 CHANGE MANAGEMENT

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	KAARTECH 's Change Management Policy requires that change requests are: • Formally documented. • Authorized • Reviewed and approved	Inspected the Change Management policy to determine that changes were: • Formally documented. • Authorized • Reviewed and approved	No exceptions noted.
CC8.1.2	Change request is logged in the service desk tool to track and document changes throughout the change management process.	Checked for the sample change requests that each request was documented, approved as per the policy requirement. It was confirmed that Network changes were not documented.	Network changes were not documented.
CC8.1.3	Network and system software patches and updates are applied to the security systems as needed.	Inquired of Management to determine whether the IT team is responsible for patch management. Inspected evidence of patch updates to determine whether the patches were applied.	No exceptions noted.
CC8.1.5	Access to move changes to the production environment is authorized and restricted to appropriate individuals to enforce segregation of duties.	Inspected the list of authorized users with access to move changes to the production environment and inquired with the management to verify that access was restricted to appropriate and authorized users.	No exceptions noted.

4.2.9 CC9.0 RISK MITIGATION

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected KaarTech Risk Assessment & Treatment register and determined whether the risk assessment is performed periodically and whether it specifies risk tolerances and includes risk identification, changes to business objectives, commitments and requirements, risk measurement, and response strategy.	No exceptions noted.
CC9.1.2	The risk management program includes insurance to minimize the financial impact of any loss events.	Inspected insurance coverages and the insurance policy to determine whether the general insurance was in place for potential loss events.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.	Inspected the sample agreements with the business partners and service providers to determine whether they included defined terms, conditions, and responsibilities of each party.	No exceptions noted.

CC9.2.2	The risk management program includes insurance to minimize the financial impact of any loss events.	Inspected insurance coverages and the insurance policy to determine whether the general insurance was in place for potential loss events.	No exceptions noted.

4.2.10 ADDITIONAL CRITERIA FOR AVAILABILITY

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
A1.1 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.			
A1.1.1	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
A1.1.2	KaarTech maintains its internal resource management tracker to keep track of all its resources and update them regularly. Resource and Capacity Management Information System reports are maintained to provide a concise view of various parameters significant to the availability of resources for continuous operations.	Inspected that Infra availability was assessed periodically.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Monitoring software identifies and evaluates ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Checked that AWS Cloudwatch tool was in use to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.

A1.2.2	KaarTech facilities are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • Uninterruptible power supply (UPS) systems • Air conditioning units Management retains the inspection report received from third-party specialists evidencing completion of inspection and maintenance periodically.	Obtained the inspection reports of air conditioning units, fire detection and suppression equipment, UPS for a sample company facility. Noted that third-party specialists performed the inspections.	No exceptions noted.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Business continuity and disaster recovery plans have been developed and updated annually.	Inspected Business Continuity Plan and Disaster Recovery Plan to determine whether plans were documented and updated annually. It was confirmed that BCP/DR test was not performed during the audit period.	BCP/DR test was not performed during the audit period.
A1.3.2	Automated backup systems are in place to perform scheduled backups of production servers at predefined times.	Inspected the back configuration and reports to determine that automated backup systems are in place to perform scheduled backups of production servers at predefined times. Checked that the backup restoration testing was performed for KEBS & Ktern.	No exceptions noted

A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Business continuity and disaster recovery plans have been developed and updated annually.	Inspected Business Continuity Plan and Disaster Recovery Plan to determine whether plans were documented and updated annually. It was confirmed that BCP/DR test was not performed during the audit period.	BCP/DR test was not performed during the audit period.
A1.3.2	Automated backup systems are in place to perform scheduled backups of production servers at predefined times.	Inspected the back configuration and reports to determine that automated backup systems are in place to perform scheduled backups of production servers at predefined times. Checked that the backup restoration testing was performed for KEBS & Ktern.	No exceptions noted.

4.2.11 ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	KaarTech has documented Data Retention Policy to ensure data protection, so that important and business critical records are protected from loss, destruction, and falsification.	Inspected the 'Data Retention Policy' to determine that it was documented to ensure data protection so that important and business-critical records are protected from loss, destruction, and falsification.	No exceptions noted.
C1.1.2	Logical and physical access controls are implemented to maintain the confidentiality of Information.	Inspected the Information Security Policy and sub-policies to determine whether logical and physical access controls were implemented to maintain the confidentiality of information.	No exceptions noted.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			

C1.2.1	Kaar Tech has documented Scrap Policy to retain and dispose of information by those policies.	Inspected that Kaar Tech - Scrap Policy to determine whether it is in place. Per inquiry with Management, no data was disposed of during the SOC review period.	No exceptions noted.

4.2.12 ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
PI1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.1.1	KaarTech is a business process management system, and all inputs, workflows, processed data, results, statuses, and output are maintained online and delivered to the client through an online user interface.	Inspected Data Retention Policy to determine whether there is a documented classification scheme for labeling and handling data, including client confidential and personal information.	No exceptions noted.
PI1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives			
It was confirmed that KAARTECH does not perform calculations on its platform.			
PI1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
PI1.3.1	All inputs, workflows, processed data, results, statuses, and output are maintained and delivered to the client through user interfaces.	Inspected the sample of the data flow process to determine that data flows according to business rules and client requirements.	No exceptions noted.
PI1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			

PI1.4.1	All inputs, workflows, processed data, results, statuses, and output are maintained and delivered to the client through user interfaces.	Inspected the sample of the data flow process to determine that data flows according to business rules and client requirements.	No exceptions noted.
PI1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives			
PI1.5.1	All inputs, workflows, processed data, results, statuses, and output are maintained and delivered to the client through user interfaces.	Inspected the sample of the data flow process to determine that data flows according to business rules and client requirements.	No exceptions noted.

4.2.13 ADDITIONAL CRITERIA FOR PRIVACY

P1.0 Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P1.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects promptly for changes to the entity's privacy practices, including changes in the use of personal			
P1.1.1	KaarTech has published policies that provide notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, quality, and monitoring of personal information.	Inspected KaarTech's privacy policy to determine whether it is documented in writing and available on the company portal.	No exceptions noted.

P2.0 Privacy Criteria Related to Choice and Consent

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P2.1 The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			

P3.0 Privacy Criteria Related to Collection

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P3.1 Personal information is collected consistent with the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			
P3.2 For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent before the collection of the information to meet the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			

P4.0 Criteria Related to Use, Retention, and Disposal

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P4.1 The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.1.1	KaarTech privacy notice indicates that the use of information is limited to the activities mentioned in the Privacy Policy.	Inspected KaarTech's privacy policy to determine whether it is documented in writing and available on the company portal. Checked that the privacy notice indicates that the use of information is limited to the activities mentioned in the Privacy Policy. Inspected service commitments and dataflow diagrams to determine that PII is not collected nor stored within the KaarTech infrastructure.	No exceptions noted.
P.2 The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.2.1	KaarTech privacy notice indicates that information will be kept for a period required to fulfill or support offered services.	Inspected the privacy policy wherein it is stipulated that the information is to be retained while the account is active and for a reasonable period following cancellation of services to allow for possible re-engagement and as required to comply with the regulatory requirements.	No exceptions noted.
P4.3 The entity securely disposes of personal information to meet the entity's objectives related to privacy.			

P4.3.1	Kaar Tech has documented Scrap Policy to retain and dispose of information by those policies.	Inspected that Kaar Tech - Scrap Policy to determine whether it is in place. Per inquiry with Management, no data was disposed of during the SOC review period.	No exceptions noted.

P5.0 Privacy Criteria Related to Access

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			
P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			

P6.0 Privacy Criteria Related to Disclosure and Notification

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
Per inquiry with Management, KaarTech does not disclose the data to any third party.			
P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
Per inquiry with Management, KaarTech does not disclose the data to any third party.			
P6.3 The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			

Per inquiry with Management, KaarTech does not disclose the data to any third party.			
P6.4 The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
Per inquiry with Management, KaarTech does not disclose the data to any third party.			
P6.5 The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's privacy objectives.			
Per inquiry with Management, KaarTech does not disclose the data to any third party.			
P6.6 The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P6.6.1	The KaarTech Incident Response Procedure plan considers notification requirements related to personal information breaches to fulfill proper communication with related parties.	Inspected the Incident Response Procedure plan to determine whether it is in place and considers notification requirements related to breaches. Per inquiry with Management, no security breaches occurred during the review period.	No exceptions noted.
P6.7 The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			

P7.0 Privacy Criteria Related to Quality

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P7.1 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
It was confirmed that KaarTech does not collect or process or store personal information from individuals for service provisioning purposes.			

P8.0 Privacy Criteria Related to Monitoring and Enforcement

Criteria	Description of KaarTech's Controls	Tests Performed by Service Auditor	Test Results
P8.1 The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
P8.1.1	KaarTech's privacy and security policies identify a process for receiving, addressing, and resolving complaints and disputes from data subjects.	Inspected the KaarTech website to determine whether it includes links for raising and documenting complaints, disputes, etc.	No exceptions noted.

SECTION 5 OTHER SUPPLEMENTAL INFORMATION

5.1 MANAGEMENT RESPONSE TO THE EXCEPTIONS NOTED

Sr. No.	Particulars	Management response
1	VAPT was not performed during the audit period.	Technically, VA cannot be performed in the production AWS cloud run time microservices environment. As per the architecture, the run time container workload OS is immutable, and the production images are deployed through CI pipeline with integrity check in place through ECR for analytics instances. w.r.t PT, black box test for FY'24-25 was completed for KEBS with the closure certificate on March '24 and for FY'25-26 both the KEBS & KTern will be initiated in the month of June – August '25.
2	The user access review for KTern was not performed.	KTern application has 4 user roles super, basic, limited and standard. Respective project owner/PMO /Customer Success Manager has "super "access and they are authorized to provide appropriate role in the KTern system as per the project requirement. The access ID are integrated with active directory and SSO enabled . Every 90 days IT department performs a review with HR team to revoke the dormant accounts from the AD. Hence compensatory control in place.
3	The firewall ruleset review was not performed during the audit period.	KaarTech does not host PCI & health industry data. Hence the mandatory half yearly firewall rule set review is not considered to meet the PCI DSS or HiTrust standard requirements. As a proactive step, vulnerable ports are kept blocked and traffic is not allowed at the perimeter level. As an opportunity for improvement, we shall put an adequate plan and execution procedure to perform half yearly ruleset review with effect from H1 '2025.
4	Network changes were not documented.	AWS hosted services network related changes are logged and recorded in AWS cloud trail. Corporate IT network related changes shall be tracked through the ticketing system with effect from June'25.
5	BCP/DR test was not performed during the audit period.	All applications are hosted in AWS. We have a contract with AWS to meet the availability & Up time. Cold site deployed for DB back up and periodic restoration test being carried out.

5.2 USER AUDITOR CONTACT

User Auditors using this report as an aid in performing their audit of user entities are encouraged to contact KaarTech or the office of ControlCase Assurance with their comments and suggestions for changes in future reports.

Comments should be forwarded to the following individuals:

Srinivasan Subbiah
Chief Information Officer
Kaar Technologies India Pvt Ltd
ssrinivasan@kaartech.com

And/or

Yusuf Musaji, CPA
Principal
ControlCase Assurance
ymusaji@controlcase.com

END OF REPORT