Frappe Technologies Private Limited SOC 2 Type II Report 2025

FRAPPE TECHNOLOGIES PRIVATE LIMITED
SOC 2 TYPE II REPORT

Report on Frappe Technologies, covering its

Product engineering, SaaS and on-premises operations

TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON

CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY, AVAILABILITY

Audit Dates: 17, 18 June 2025

Audit Period: 01st June 2024 to 31st May 2025

This report is intended solely for compliance purposes and for use by the management of Frappe Technologies, user entities of Frappe Technologies services, and other parties who possess sufficient knowledge and understanding of the services covered herein (each, a “specified user”).

If the report recipient is not a specified user (hereinafter a “non-specified user”), any use of this report is solely at the non-specified user’s own responsibility and risk. Non-specified users may not rely on this report and do not acquire any rights against Quality Asia or the service auditor by virtue of access thereto. Furthermore, neither Quality Asia nor the service auditor assumes any duty or obligation to any non-specified user who obtains this report or accesses any part thereof.

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

Table of Contents

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To Director,

Frappe Technologies.

Scope

We have examined Frappe applies to information assets utilized for product engineering and operations lifecycle for on-premises and SaaS based product offerings and the support functions like Infra, HR, Legal, Revenue, Customer Support & Admin operating—covering the period from 01 June 2024 to 31 May 2025 (the "Description"). We evaluated the suitability of the design and operating effectiveness of controls to meet Frappe Technologies's service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity, and Privacy as outlined in TSP Section 100 Principles and Criteria, and the applicable Trust Services Criteria for Security, Confidentiality, and Availability, for the period from 01 June 2024 to 31 May 2025.

Frappe Technologies utilizes Amazon Web Services Inc. (AWS) for its IT infrastructure and platform services. The Description outlines Frappe Technologies's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of these controls. The Description does not disclose the actual controls implemented at subservice organizations. Our examination did not include the services provided by subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Similarly, the Description presents Frappe Technologies's controls, the applicable Trust Services Criteria, and the types of complementary user entity controls assumed in the design of these controls. The Description does not disclose the actual controls at the user entity organizations. Our examination did not include the services provided by the user entity organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities.

Frappe Technologies has provided the accompanying management assertion titled "Frappe Technologies, Assertion for the Period 01 June 2024 to 31 May 2025" regarding the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls described therein to meet Frappe Technologies service

commitments and system requirements based on the applicable Trust Services Criteria. Frappe Technologies is responsible for:

- (1) preparing the Description and assertion.
- (2) ensuring the completeness, accuracy, and method of presentation of the Description and assertion.
- (3) delivering the digital services covered by the Description.
- (4) identifying risks that might prevent the applicable Trust Services Criteria from being met.
- (5) specifying the controls that meet Frappe Technologies service commitments and system requirements based on the applicable Trust Services Criteria and detailing them in the Description; and
- (6) designing, implementing, maintaining, and documenting controls to meet Frappe Technologies service commitments and system requirements based on the applicable Trust Services Criteria stated in the Description.

Service Auditor's responsibilities.

Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the description criteria set forth in Frappe Technologies assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that Frappe Technologies service commitments and system requirements were met based on the applicable Trust Services Criteria.

We conducted our examination in accordance with the attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- (1) the Description is fairly presented based on the description criteria.
- (2) the controls were suitably designed to provide reasonable assurance that Frappe Technologies service commitments and system requirements would be achieved if the controls operated effectively based on the applicable Trust Services Criteria; and
- (3) the controls operated effectively to provide reasonable assurance that Frappe Technologies service commitments and system requirements were achieved based on the applicable Trust Services Criteria throughout the period from 01 June 2024 to 31 May 2025.

Our examination involved performing procedures to obtain evidence regarding the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to meet the applicable Trust Services Criteria. Our procedures included assessing the risks that the Description might not be fairly presented and that the controls were not suitably designed or operating effectively to provide reasonable assurance that Frappe Technologies service commitments and system requirements met the applicable Trust Services Criteria. Additionally, our procedures included testing the operating effectiveness of those controls deemed necessary to provide reasonable assurance that Frappe Technologies's commitments and system requirements were met. We also evaluated the overall presentation of the Description. We believe that the evidence obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that an individual user might consider important for its needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable Trust Services Criteria. Furthermore, any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design of the controls to meet the applicable Trust Services Criteria is subject to the risk that the system may change or that controls at a service organization may become inadequate or fail.

Description of tests of controls

In Section III, the specific controls evaluated, along with the nature, timing, and results of those tests, are detailed in the accompanying "Description of Criteria, Controls, Tests, and Results of Tests."

Opinion

In our opinion, in all material respects, based on the description criteria described in Frappe Technologies assertion and the applicable Trust Services Criteria:

- The Description fairly presents the system that was designed and implemented throughout the period from 01 June 2024 to 31 May 2025.
- The controls stated in the Description were suitably designed to provide reasonable assurance that Frappe Technologies service commitments and system requirements would be achieved if the controls operated effectively based on the applicable Trust Services Criteria, and if subservice organizations and user entities applied the controls

contemplated in the design of Frappe Technologies controls throughout the period from 01 June 2024 to 31 May 2025.

- The controls tested, which were those necessary to provide reasonable assurance that Frappe Technologies service commitments and system requirements based on the applicable Trust Services Criteria were met, operated effectively throughout the period from 01 June 2024 to 31 May 2025.

Restricted Use

This report, including the description of tests of controls and the results thereof as presented in the "Description of Tests and Results," is intended solely for the use of the user entities of Frappe Technologies system for the period from 01 June 2024 to 31 May 2025, prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the digital services provided by Frappe Technologies.
- How Frappe Technologies system interacts with user entities, subservice organizations, or other parties, including the internal controls and their limitations.
- The complementary controls in place at subservice organizations and the user entity controls, and how those controls interact with the controls at Frappe Technologies to achieve its service commitments and system requirements.
- The applicable Trust Services Criteria.
- The risks that may threaten the achievement of the applicable Trust Services Criteria and how the controls address those risks.

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

Sirsa Ghosh

Certified Public Accountant

SIRSA GHOSH

License No. 6298

SECTION 2

Management's Assertion

Management's Assertion

Frappe Technologies Management Assertion for the Period 01 June 2024 to 31 May 2025

We have prepared the accompanying description of the Frappe Technologies Platform (hereafter "the Platform"), which details our comprehensive digital services and integrated FinOps management solution, for the period from 01 June 2024 to 31 May 2025 (the "Description"). This Description has been developed in accordance with the criteria specified in items (a)(I)–(ii) below, establishing the requirements for describing a service organization's system as outlined in DC Section 200 by the AICPA's Assurance Services Executive Committee and its Trust Information Integrity Task Force's SOC 2 Guide Working Group. The Description is intended to provide our specified users with critical insights into the system and infrastructure offered by the Platform, thereby enabling an informed assessment of the risks associated with interactions during the stated period. It addresses the suitability of the design and operating effectiveness of controls to meet our service commitments and system requirements based on the criteria for Security, Confidentiality, and Availability (the applicable trust services criteria) as set forth in TSP Section 100 and the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The Platform leverages Amazon Web Services Inc. (AWS) as a subservice organization for hosting its production systems and securely storing customer data. The Description indicates that effective complementary controls at subservice organizations are required, in conjunction with the controls implemented by Frappe Technologies Platform, to achieve our service commitments and system requirements under the applicable trust services criteria. Accordingly, the Description outlines our controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of these controls, without disclosing the actual controls implemented by these subservice organizations.

Similarly, the Description highlights that effective complementary controls at user entity organizations are necessary—alongside the controls maintained by Frappe Technologies Platform—to satisfy our service commitments and system requirements based on the applicable trust services criteria. The Description presents our controls, the applicable trust services criteria, and the types of complementary user entity organization controls assumed in the design of these controls, without disclosing the actual controls implemented at the user entity organizations.

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

- The Description fairly presents the Frappe Technologies Platform, and the services delivered through it as designed and implemented throughout the period from 01 June 2024 to 31 May 2025. The criteria for the Description are identified below under the heading "Description Criteria."

- The controls described were suitably designed and operated effectively to meet the Platform's service commitments and system requirements in accordance with the applicable trust services criteria throughout the period from 01 June 2024 to 31 May 2025.

Description Criteria:

- The description contains the following information:
  - The types of services provided.
  - The principal's service commitments and system requirements
- The components of the system used to provide the services, which are the following:
  - Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
  - Software. The programs and operating software of a system (systems, applications, and utilities).
  - People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
  - Procedures. The automated and manual procedures involved in the operation of a system.
  - Data. The information used and supported by a system (transaction streams, files, databases, and tables).
  - The boundaries or aspects of the system covered by the description.
  - The applicable trust services criteria and the related controls are designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.
  - Other aspects of the service organization's control environment, risk assessment process, communication and information systems and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
  - The description does not omit or distort information relevant to the service organizations' system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore include every aspect of the system that each individual user may consider important to his or her own needs.
  - Frappe Technologies has determined that Processing Integrity and Privacy trust services Categories are not relevant to the system.

Frappe Technologies

Authorized Signatory

SECTION 3

Description of the System

Description of the System

1. Overview of Operations

1.1. Description of Services Provided

Frappe Technologies is a technology-driven company specializing in digital transformation, cybersecurity, IT infrastructure management, and cloud solutions. We provide tailored digital solutions to enhance security, efficiency, and business continuity. Our key services include:

- Cybersecurity Solutions – Implementing robust security frameworks, risk assessments, and compliance with international standards such as ISO 27001.
- IT Infrastructure Management – Offering seamless network management, cloud computing solutions, and data protection strategies.
- Digital Transformation – Helping businesses adopt the latest technologies, including AI-driven automation, data analytics, and ERP system integrations.
- Software Development & Custom Solutions – Developing enterprise-grade applications, web platforms, and mobile apps.
- Consulting & Compliance – Assisting organizations in meeting regulatory and compliance standards for data protection, cybersecurity, and business process optimization.

Frappe Technologies Vision

We aspire to build great products and services, empower and educate, and be a democratically run organization.

Frappe Technologies Mission

Our mission is to provide its operational ethos and strategic initiatives reflect a commitment to:

- Excellence in Product Development.
- Empowerment through Open Source.
- Democratic Organizational Structure.

Frappe Technologies's Core Values

These values define the culture at Frappe Technologies and drive all aspects of its strategy, operations, and interactions with the community and customers Delivering highly secure and compliant IT infrastructure solutions.

- Excellence: Commitment to building high-quality, user-centric, and scalable open-source products.

- Teamwork: Prioritizing collective success over individual achievements through collaboration and mutual support.
- Authenticity: This value summarizes various ideas like sustainability, simplicity, originality, honesty, minimalism, thrift, conscious consumption.

Principal Service Commitments and System Requirements

Frappe Technologies LLP designs its processes and procedures related to its systems to meet its service objectives. These objectives are based on the commitments made to user entities, the laws and regulations governing their services, and the financial, operational, and compliance requirements established by Frappe Technologies. The company ensures that its systems align with security, confidentiality, and availability commitments, which are formally documented in Service Level Agreements (SLAs) and other contractual agreements.

The security, confidentiality, and availability of the system are governed by setting up internal controls and industry best practices. The following commitments form the foundation of Frappe Technologies approach to system integrity and risk management.

Security Commitments

Frappe Technologies is committed to ensuring the security of its systems and data by implementing stringent measures, including but not limited to:

- Role-Based Access Control (RBAC): Users can access system resources based on their designated roles, ensuring minimal privilege access and preventing unauthorized access.
- Infrastructure & Environment Controls: Strict access controls are in place for the production environment and supporting infrastructure to mitigate risks related to unauthorized modifications.
- Continuous Monitoring: Key infrastructure components are monitored in real-time to generate alerts based on utilization metrics and potential security threats.
- Regular Security Assessments: Periodic vulnerability scans, penetration testing, and risk assessments are conducted to identify and address security gaps proactively.
- Incident Response & Breach Management: Clearly defined incident response procedures ensure that security incidents are detected, managed, and resolved effectively, with timely notifications to stakeholders.

Confidentiality Commitments

Frappe Technologies enforces strict confidentiality measures to protect sensitive business and customer data, including:

- Data Encryption: Sensitive system data is encrypted both at rest and in transit using industry-standard encryption protocols.
- Confidentiality Agreements: All employees, contractors, and third parties must sign confidentiality and non-disclosure agreements (NDAs) before handling sensitive information.
- Access Restrictions: Confidential information is strictly used for the purposes explicitly stated in agreements between Frappe Technologies and user entities, ensuring compliance with data privacy regulations.

Availability Commitments

Frappe Technologies ensures high system availability and performance through robust operational procedures, including:

- System Performance & Uptime Monitoring: Automated monitoring systems track uptime and performance metrics to ensure continuous service availability.
- Customer Support & Response: Customer requests are processed in a timely and efficient manner in accordance with SLA commitments.
- Business Continuity & Disaster Recovery: A comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) outline the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) to mitigate downtime risks.
- Operational Resilience: Standardized procedures support proactive maintenance and rapid recovery in case of service disruptions.

These commitments are formally communicated in Frappe Technologies policies and procedures, system design documentation, and customer contracts. The company's Information Security Management System (ISMS) defines an organization-wide approach for data protection, system operations, business continuity, and employee training. Standard operating procedures are documented to ensure consistency in manual and automated processes supporting system security and compliance.

Components of the System used to provide services.

To define the system boundaries, service commitments, and internal controls in place for delivering Frappe Technologies' services, including ERP Next, Frappe Cloud, and allied digital solutions. The system is categorized into five key components: infrastructure, software, people, data, and processes and procedures.

Infrastructure

Frappe Technologies' production environment is hosted on Frappe Cloud, leveraging AWS and Digital Ocean infrastructure in a hybrid deployment model. This environment is engineered for high performance, availability, redundancy, and secure data isolation.

Key Infrastructure Controls:

- Virtual Private Cloud (VPC): All deployments are containerized within isolated VPCs.
- Access Controls: Firewall rules and ingress filtering restrict access only to designated entry points.
- Encrypted Transmission: All communications are secured using TLS 1.2+ HTTPS protocols.
- Monitoring & Intrusion Detection: Centralized logging and monitoring tools (e.g., Fail2Ban, Sentry, Prometheus) detect anomalies and potential breaches.
- Backup & Disaster Recovery: Automated daily backups and geo-redundant storage ensure availability.

Software

Frappe develops, maintains, and delivers its proprietary applications using open-source technologies integrated into a secure CI/CD pipeline.

Key Software Components:

- ERP Next: Cloud-native, modular ERP system based on the Frappe Framework.
- Frappe Framework: Metadata-driven development framework using Python, MariaDB, and Redis.
- Database Systems: Managed MariaDB and Redis instances for relational and cache data.
- Containerization & Orchestration: Docker and Kubernetes-based deployment.
- Security Layers: API rate limiting, role-based access, OAuth2 authentication, and CSRF/XSS protection.

People

Operations are maintained by skilled professionals across DevOps, engineering, support, and compliance.

Personnel Controls:

- Role-Based Access Control (RBAC): Roles defined by least-privilege principles.
- Authentication Measures: Multi-Factor Authentication (MFA) is enforced on all admin interfaces.
- Training & Awareness: Cybersecurity and data protection awareness sessions held quarterly.
- Verification: Background verification, confidentiality agreements, and code-of-conduct compliance for all employees.

Data

Frappe handles both operational and client data in compliance with GDPR, ISO 27001, and SOC 2 principles.

Data Types and Security Controls:

- Customer Data: Encrypted in-transit and at rest using AES-256 encryption.
- Operational Data: Includes logs, metrics, audit trails for diagnostic and forensic use.
- Access Logs & Authentication Data: Managed via OAuth2, 2FA, and LDAP/SAML where applicable.

Data Classification & Handling:

- Confidential: Stored in encrypted volumes with restricted access.
- Internal Use: Accessible within authorized project scopes only.
- Public: Approved documentation and product information available via official channels.

Data Sensitivity	Store and use	Share
Confidential	Labelled and handled as "Confidential". Stored in secure, access-controlled environments (encrypted cloud folders or internal repositories). Access is restricted to authorized personnel based on role-based access control (RBAC).	• Not to be shared or displayed to unauthorized individuals without explicit approval from the Chief Executive or Data Protection Officer (DPO) • Sharing permitted only among senior or designated personnel within the organization with logged authorization.

Internal	Classified as internal business or operational data. Stored on company-controlled infrastructure or cloud services with restricted internal access	• Not to be shared externally beyond Frappe Technologies' operational scope. • Requires documented approval from the Security & Compliance Lead or relevant Functional Head before any external disclosure.
Public	Official documents, marketing content, blogs, open-source repositories (e.g., ERPNext GitHub), and other approved content. Stored on publicly accessible platforms or Frappe.io.	• Freely shareable without prior approvals. • Dissemination via official communication channels is encouraged to maintain brand consistency.

Processes and Procedures

Formal policies and procedures have been established to support the Frappe Technologies, these policies & procedure cover:

- WFH Security Guidelines
- Business Code of Conduct
- Prevention of Sexual Harassment Policy
- Confidentiality Policy
- Policy Document Control
- Admin Procedure
- Customer Support Procedure
- Development Manual
- BYOD Procedure
- Legal Procedure
- Risk Assessment & Treatment Methodology
- Release Manual
- Sales Manual
- Access Control Process
- Antivirus Management Process
- Control of Documented Information Process
- Cyber Security/Infosec Awareness Process

- Data Leakage Prevention Process
- Human Resource Security Management Process
- IT Media Management Process
- Network Security Management Process
- Project Management Process
- Software Installation Process
- Vendor Management Process
- Change Management Process
- Asset Management Process
- Backup & Restoration Process
- Business Continuity Management Process
- Logging & Monitoring Process
- Patch Management Process
- Cryptography & Key Management Process
- Vulnerability Management Process
- Password Management Process
- Threat Intelligence Management Process
- Information Security Incident Management Process
- Compliance Management Process
- Capacity Management Process
- Configuration Management Process
- Acceptable Usage of Assets
- Cloud Security Management Process
- Frappe Endpoint Security Process
- Customer Satisfaction Management Process
- Knowledge Management Process
- HR & Training Management Process
- Corrective Action & Improvement Process
- Risk & Opportunity Management Process
- Vendor Risk Management Process
- Information Classification & Labelling Process

These components work together to support Frappe Technologies service commitments, ensuring the security, confidentiality, and availability of customer data and services.

All policies are made accessible to all staff members, ensuring they understand their roles and responsibilities related to internal controls and service delivery. Employees are required to comply with these policies and procedures, which define best practices for delivering services securely and efficiently. Each staff member must acknowledge their understanding of these policies upon hiring and annually thereafter as part of compliance and training initiatives.

Frappe Technologies provides clear reporting channels for clients and staff members to report failures, security incidents, concerns, or complaints related to its services and systems. Upon receiving a report, Frappe Technologies promptly investigates and takes appropriate action within a defined response timeframe, ensuring minimal disruption to business operations.

Control Environment, Risk Assessment, Information & Communication, and Monitoring

Frappe Technologies LLP evaluates the suitability, design, and operational effectiveness of its controls using the applicable Trust Services Criteria. These criteria, along with their associated controls, are detailed in Section IV of this report but remain an integral part of the overall system description.

This section outlines five key components of internal control at Frappe Technologies:

- Control Environment: Establishing a culture of security, compliance, and ethical responsibility.
- Risk Assessment: Identifying, evaluating, and mitigating potential security and operational risks.
- Control Activities: Implementing preventive, detective, and corrective controls to safeguard information systems.
- Information & Communication: Ensuring transparent and secure communication across internal teams and external stakeholders.
- Monitoring Controls: Conducting continuous assessments, audits, and reviews to maintain system integrity and compliance.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and check them. Integrity and ethical values are essential elements of Frappe Technologies control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Frappe Technologies ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

Frappe Technologies management team has set up the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members must acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Frappe Technologies management defines competence as the knowledge and skills necessary to carry out tasks that define employees' roles and responsibilities. The following controls have been set up to incorporate commitment to competence throughout the organization:

- The management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by senior management.
- Annual Security Awareness Training is provided for all staff, which focuses on keeping the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Senior Management Oversight

Frappe Technologies control awareness is significantly influenced by its senior management. Attributes that define "tone at the top" include senior management's experience of its members, their involvement and scrutiny of operational activities, and their inter-action with independent assessments of the company's operations and information security posture.

Management Philosophy and Operating Style

Frappe Technologies management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information. Frappe Technologies control environment reflects the philosophy of management. Frappe Technologies information security function, composed of senior management and the Information Security Officer, meets often and includes at least an annual

meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities Frappe Technologies has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business.
- Senior management reviews the functioning of internal controls, supplier risk assessment, risk assessment, and high severity security incidents annually.
- Senior management meets often and includes at least an annual meeting to review policies and procedures and set up the information security program roadmap.

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

Human Resources

Frappe Technologies success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is shown by the management's ability to hire and retain top quality personnel who ensure the service

organization operates at maximum efficiency. Specific control activities that the service organization has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees must acknowledge company policy and confidentiality-related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies or otherwise acts in a manner considered contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

Risk Assessment

Frappe Technologies follows a proactive risk management approach to identify, evaluate, and mitigate potential security, operational, and compliance risks that may impact its services. The organization conducts regular risk assessments to address internal and external threats, ensuring alignment with industry best practices and regulatory requirements.

Key aspects of Frappe Technologies risk assessment process include:

- Threat Identification: Evaluating potential risks, including cyber threats, data breaches, system failures, insider threats, and third-party vulnerabilities.
- Impact Analysis: Assessing the potential impact of identified risks on service availability, confidentiality, and system integrity.
- Risk Mitigation Strategies: Implementing preventive, detective, and corrective controls to minimize risks and ensure business continuity.
- Continuous Monitoring: Using automated tools, periodic security audits, and penetration testing to detect vulnerabilities and improve security posture.
- Regulatory Compliance: Ensuring adherence to SOC 2, ISO 27001, GDPR, and other relevant compliance frameworks to maintain a secure and trustworthy environment.

Frappe Technologies risk assessment framework is reviewed periodically and updated as needed to address evolving threats and technological advancements.

Scope

The risk assessment and management program at Frappe Technologies applies to all systems, data, and operational processes within the organization. The risk assessment process evaluates critical infrastructure components, including:

- Computer networks and cloud environments
- Instances, databases, and storage systems
- Business and IT practices, policies, and physical security measures

Risk assessments may be conducted at a high level or may be detailed for specific organizational or technical changes, depending on the needs of stakeholders and technical teams.

The execution, development, and implementation of risk assessments and remediation plans are a shared responsibility between:

- The Information Security Officer, who oversees the risk assessment framework
- Department heads and responsible personnel, who assist in the assessment of their respective areas

All Frappe Technologies employees are expected to:

- Cooperate fully with risk assessments related to systems, processes, and data under their control
- Collaborate with the risk assessment project led to develop an appropriate remediation plan when risks are identified

Vendor Risk Assessment

Frappe Technologies relies on third-party vendors to meet its business and operational objectives. Recognizing the inherent risks in vendor relationships, Frappe Technologies actively monitors and evaluates vendor-related risks to protect its systems, data, and business commitments.

Key vendor risk management activities include:

- Annual Vendor Risk Assessment: The Information Security Officer conducts an annual review of vendor relationships, assessing potential security, compliance, and operational risks.
- Compliance Verification: For critical vendors, Frappe Technologies reviews third-party security assessments and compliance reports (e.g., SOC 2, ISO 27001, GDPR) to ensure alignment with its security commitments.

- Periodic Vendor Reviews: If a critical vendor does not provide a third-party security report, Frappe Technologies's management meets with them periodically to assess performance, security concerns, and service reliability.
- Risk Documentation & Review: Identified vendor risks are recorded in a Risk Assessment Matrix, which is reviewed annually by senior management.

Integration with Risk Assessment

As part of its risk management strategy, Frappe Technologies LLP:

- Identifies risks that could impact its ability to meet service commitments
- Implements controls to mitigate those risks effectively
- Performs an annual risk assessment to evaluate:
    - Internal and external threats
    - Potential business impact and likelihood of risks
    - Severity of risks and necessary mitigation actions

Frappe Technologies LLP continuously enhances its risk management framework to ensure business continuity, security, and regulatory compliance.

Control Activities

Frappe Technologies' control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's aims. Such statements may be documented, explicitly said in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that set up what is expected and procedures that put policies into action.

Logical Access Control

Frappe Technologies uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application, and authenticates to the database.

Frappe Technologies has identified certain systems that are critical to meeting its service commitments. All access to control systems is under the principle of the least required privilege (wherein a staff member is granted the minimum necessary access to per-form their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a

person is relieved of duties from the company, access to critical systems is revoked with immediate effect as per policies.

Administrators' access to the production console is restricted to authorized system and security administrators. Powerful ser-vice/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

Frappe Technologies handles performing regular reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least- privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all their accounts that have access to Frappe Technologies customer data. Staff are encouraged to use passwords which have at least 10 characters, randomly generated, alphanumeric and special character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems require multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted on AWS. As such, AWS handles the physical security controls of the in-scope system. Frappe Technologies reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are by standards expected by the customers of the Frappe Technologies system.

Incident Management

Procedures for incident response, including the identification and escalation of security breaches and other incidents, are outlined in the Incident Management Policy. Incidents and complaints are reported via email and recorded in the ISMS portal within the Confluence tool. When an incident is detected or reported, authorized personnel start a defined incident response process. Incidents are assigned a priority level (high, medium, or low) based on impact, urgency, and business criticality, as decided by the initiator or incident manager. Corrective actions are implemented according to defined policies and procedures. Tickets are raised for recurring high-priority incidents, and a Root Cause Analysis (RCA) is conducted to identify a permanent solution for these tickets.

Network Operations Monitoring

Access to production instances is protected by deploying network security groups that inspect traffic flowing to cloud virtual resources for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between virtual network environments to ensure that only authorized systems can communicate with other systems necessary to fulfil their specific responsibilities.

Operations and security functions utilize a variety of security tools to identify and detect potential security threats and incidents. These tools include, but are not limited to, log notifications, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from security tools are reviewed by Frappe Technologies management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

Frappe Technologies only allows network ports, protocols, and services that have a validated business need to operate on each system. Default-deny rules block all traffic except for explicitly allowed services and ports.

Cryptography

User requests for Frappe Technologies's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to Frappe Technologies web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

Change Management

Requirements for software development are obtained from the client business owners. These requirements are documented as Software Requirement Specifications (SRS)/User Stories. The requirements are baseline, and whenever there is a change to the baseline, the relevant stakeholders review the impact of the change. The changes are prioritized based on the available capacity in the road map plan. The change management process is documented and communicated with the client promptly. Ap-proved changes are added, and a new baseline version is created. Change management is applied at the resource level for projects where Frappe Technologies is only responsible for providing personnel for software development services.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Frappe Technologies uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technological assets with the potential to store or process information is maintained.

Vulnerability and Patch Management

A patch management procedure is developed in discussion with user SMEs, starting with documenting all the inventory of the production systems. An impact analysis is performed on the outdated versions, and a plan is developed to update the software versions necessary for production systems. Patches are applied in the production systems as agreed with the user entities, followed by evaluating the updated patches. A rollback plan is also included if the test fails. Once the testing is successful and all end results are validated, sign-off is obtained from the user entities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, BYOD Bring-your-own devices is permitted and is controlled as per BYOD policy that could connect to or access data within the system boundaries. Policies enforced on endpoints include MDM, Anti-Malware and encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

Frappe Technologies has a documented business continuity plan (BCP), and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Information and Communication

Frappe Technologies maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Frappe Technologies also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet. Information about the system and services is maintained and made available to users on the company website.

Monitoring Controls

Frappe Technologies's management monitors to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Disclosure of Incidents

There were no system incidents as of 01 June 2024 to 31 May 2025, requiring disclosure that either: were the result of controls failing; or, resulted in a significant impairment to the achievement of system requirements or service commitments to customers.

Complementary User Entity Controls

Frappe Technologies's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for the processing of transactions for Frappe Technologies's customers.

For customers to rely on the information processed through the Frappe Technologies's developed software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the software application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access.
- User entity is responsible for removing terminated employee access.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the software application.
- User entity is responsible for sending data to software application via a secure connection and/or the data should be encrypted.
- User entity is responsible for notifying Frappe Technologies if they detect or suspect any security incident related to Frappe Technologies services.
- User entity is responsible for reviewing email and other forms of communications from Frappe Technologies, related to changes that may affect Frappe Technologies customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system- generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own business continuity and disaster recovery plan.

Trust Services Criteria Not Relevant to this Examination

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

- 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 communicative 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 a correction.
- Disclosure and Notification. The entity discloses personal information with the consent of the data subjects. 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.

Complementary Subservice Organization Controls

Frappe Technologies uses subservice organizations in support of its system. Frappe Technologies's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Frappe Technologies to be achieved solely by Frappe Technologies Therefore, user entity controls must be evaluated in conjunction with Frappe Technologies's controls de-scribed in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Frappe Technologies periodically reviews the quality of the outsourced operations by various methods including:

Trust Services Criteria Not Relevant to this Examination

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

- 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 communicative 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 a correction.
- Disclosure and Notification. The entity discloses personal information with the consent of the data subjects. 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.

Complementary Subservice Organization Controls

Frappe Technologies uses subservice organizations in support of its system. Frappe Technologies's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Frappe Technologies to be achieved solely by Frappe Technologies Therefore, user entity controls must be evaluated in conjunction with Frappe Technologies's controls de-scribed in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Frappe Technologies periodically reviews the quality of the outsourced operations by various methods including:

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and		CC6.1,

virtualization management software for cloud architecture is appropriate.	AWS	CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	AWS	CC6.4, CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS	CC6.4, A1.2
Business continuity and disaster recovery procedures are developed, reviewed, and evaluated periodically.	AWS	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS	A1.2
A defined process is in place to sanitize anddestroy hard drives and back up media containing customer data prior to leaving company facilities.	AWS	C1.2

SECTION 4

Testing Matrices

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Frappe Technologies' systems provided by Frappe Technologies. The scope of the testing was restricted to the Frappe Technologies system, and its boundaries as defined in Section 3. Quality Asia conducted examination testing for the observation period from 01 June 2024 to 31 May 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, we considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	I inquired about relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, ora combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Quality Asia utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Quality Asia, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including, but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted” in the test result column of the Testing Matrices. Any phrase other than the afore mentioned constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

About the CPA

This report has been prepared and issued by **Sirsa Ghosh**, a **Certified Public Accountant (CPA)**, holding **License No. 6298**. The CPA has conducted the examination in accordance with the applicable auditing standards to provide an independent assessment of Frappe Technologies’s controls relevant to the scope of this report.

The auditor’s responsibility is to express an opinion on the fairness of the presentation and the effectiveness of controls in place, ensuring alignment with SOC 2 Type II requirements.

Security Principle and Criteria Table

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: CONTROL ENVIRONMENT			
CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Entity establishes behavioral standards which are defined in the Code of Conduct and makes it available to all staff members on the company intranet.	Inspected the Code of conduct. Available on the company intranet. Frappe Business Code of Conduct V4.0	No exceptions noted.
CC1.1.2	The entity requires that new employees review and acknowledge the Code of Conduct upon hire, and that all staff members review and acknowledge it annually.	Inspected the Code of conduct. It has been reviewed and acknowledged by staff members annually. Employee Acknowledgment – Code of Conduct	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	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and Approved by Senior Management. Frappe Control of Documented Information Process V1.0	No exceptions noted.
CC1.2.2	Entity's Senior Management reviews and approves the Internal Audit Assessment report annually.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC1.2.3	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the Organizational Chart for all employees. Has been reviewed and approve by Senior. Management. Organization Chart	No exceptions noted.
CC1.2.4	The Entity’s Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. The same has been reviewed and approved by Senior Management. Approval Record	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.5	The Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Risk Assessment Report. The same has been reviewed and approved by Senior Management. Approval Record	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	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	Inspected the Organizational Structure. They maintain authorities, facilitate information flow, and establish responsibilities. No noted exceptions. Organization Chart	No exceptions noted.
CC1.3.2	Entity maintains job descriptions for clients serving IT and engineering positions to increase the operational effectiveness of employees within the Organization	Inspected the Job Descriptions. Competence Matrix	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	Entity ensures that new hires have been duly evaluated for competence in their expected job responsibilities.	Observed the Competence Evaluation for New Hires. Competency Record	No exceptions noted.
CC1.4.2	Entity ensures that new hires go through a background check as part of their onboarding process.	Background verification and vendor management processes are defined, but contractual clauses (data return/deletion and control measures) and annual performance reviews should be consistently evidenced.	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	Entity has established an Information Security Awareness training, and its contents are available for all staff on the company intranet.	Inspected the Information Security Awareness Deck. Cyber Security/Infosec Awareness Process	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Information Security Awareness Training	
CC1.5.2	The entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.	Observed the Information Security Awareness training records for 2025 Information Security Awareness Training	No exceptions noted.
CC1.5.3	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibility-ties.	Observed the periodical evaluation of job responsibilities. Document review	No exceptions noted.
CC1.5.4	Entity requires that all staff members review and acknowledge company policies annually.	New Policies will be available as newsletters for the employee to acknowledge. Evidence	No exceptions noted.
CC2.0: COMMUNICATION AND INFORMATION			
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	The entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC2.1.2	Entity makes all policies and procedures available to all staff members via the company intranet.	Document Published on the Spaces – Gameplan Evidence	No exceptions noted.
CC2.1.3	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the current information about its services on the website. frappe.io/	No exceptions noted.
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	Entity establishes behavioral standards which are defined in the Code of Conduct and makes it available to all staff members on the company intranet.	Inspected the behavioral standards in the Code of Conduct. Frappe Business Code of Conduct_V4.0	No exceptions noted.
CC2.2.2	The entity requires that new staff members complete Information Security Awareness training upon	Observed the annual Security Awareness training records.	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	hire, and that all staff members complete Information Security Awareness training annually.	Cyber Security/Infosec Awareness Process Information Security Awareness Training	
CC2.2.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Employee Acknowledgment – Code of Conduct	No exceptions noted.
CC2.2.4	Entity makes all policies and procedures available to all staff members via the company intranet.	Document Published on the Spaces – Gameplan Evidence	No exceptions noted.
CC2.2.5	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the Information Security Policy. Document Published on the Spaces – Gameplan Evidence	No exceptions noted.
CC2.2.6	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to follow them.	Inspected the company policies. Employee Acknowledgment – Code of Conduct	No exceptions noted.
CC2.3: COSO Principle 15: The entity communicates with external parties about matters affecting the functioning of internal control.			
CC2.3.1	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the current information about its services on the website. frappe.io/	No exceptions noted.
CC2.3.2	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the Information Security Policy. Ticketing tool being used for the Customer complaint – filter used for separating the low feedback Evidence	No exceptions noted.
CC3.0: RISK ASSESSMENT			
CC3.1: COSO Principle 6: The entity specifies aims with sufficient clarity to enable the identification and assessment of risks relating to objectives.			

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.1	Entity has formally documented policies and procedures to govern risk management.	Observed the annual formal risk assessment exercise records. Risk & Opportunity Management Process Risk Assessment and Treatment Methodology V4.0	No exceptions noted.
CC3.1.2	Entity performs a formal risk assessment exercise annually, as de-tailed out in the Risk Assessment and Management Policy, to find threats that could impair systems' security commitments and requirements	Observed the annual formal risk assessment exercise records. Risk Assessment	No exceptions noted.
CC3.2: COSO Principle 7: The entity finds 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	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to find threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records. Risk Assessment	No exceptions noted.
CC3.2.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all risk.	Observed the risk mitigating factors. Risk Assessment	No exceptions noted.
CC3.2.3	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to follow them.	Inspected the company policies. It has been reviewed and acknowledged by new staff members. Employee Acknowledgment – Code of Conduct	No exceptions noted.
CC3.2.4	Entity performs a formal supplier risk assessment exercise annually, as detailed out in the Risk Assessment and Management Poli-cy, to find suppliers that are critical to the systems' security commitments and requirements.	Observed the annual formal supplier risk assessment exercise records. Risk Assessment	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of aims.			

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.1	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Observed the risk matrix records. Risk Assessment	No exceptions noted.
CC3.4: COSO Principle 9: The entity finds and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment annually, as detailed out in the Risk Assessment and Management Policy, to find threats that could impair systems' security commitments and requirements	Observed the annual formal risk assessment exercise records. Inspected the Risk Assessment and Management Policy. Risk Assessment	No exceptions noted.
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all the risk.	Observed the risk mitigating factors. Risk Assessment	No exceptions noted.
CC3.4.3	Entity performs a formal supplier risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to find supplier that are critical to the systems' security commitments and requirements	Observed the annual formal risk assessment exercise records. Risk Assessment	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to find whether the components of internal control are present and functioning.			
CC4.1.1	Entity's Senior Management assigns the role of In-formation Security Officer who is delegated the responsibility of planning, assessing, implementing and re-viewing the internal control environment.	Inspected the planning, assessing, implementing, and internal control environment. ISMS Roles & Responsibilities	No exceptions noted.
CC4.1.2	Entity appoints an owner of Infrastructure, who handles all assets in the inventory.	Inspected Infra Operations Person document. A dedicated person is responsible for all assets in the inventory. Asset Master File Verified.	No exceptions noted.
CC4.1.3	Entity uses a continuous monitoring system, to track and	Inspected the monitoring tool that	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	report the health of the information security program to the Information Security Officer and other stakeholders	continuously tracks and reports the health of the information security program.	
CC4.1.4	Entity's Senior Management reviews and approves all company policies annually.	Inspected the annual company policy review.	No exceptions noted.
CC4.1.5	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the MRM minutes confirming review and approval. April 2025- MRM Minutes	No exceptions noted.
CC4.1.6	Entity's Senior Management reviews and approves the Organizational Chart annually.	Inspected the Organizational Chart review records. Organization Chart V.4.0	No exceptions noted.
CC4.1.7	The Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report confirming review and approval. Approval Record	No exceptions noted.
CC4.1.8	The Entity's Senior Management reviews and approves the "supplier Risk Assessment Report" annually.	Inspected the Supplier Risk Assessment Report confirming review and approval. Approval Record	No exceptions noted.
CC4.1.9	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Observed subservice organization reviews in the system.	No exceptions noted.
CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the security policy shared with all employees. Information Security Incident Management Process V4.0	No exceptions noted.
CC4.2.2	Entity's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and	Inspected the internal audit assessment report.	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	shares the findings in an "Internal Audit Assessment" report with Senior Management.	It has been reviewed and approved by Senior Management. Internal Audit Checklist	
CC4.2.3	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies confirming review and approval. Frappe Control of Documented Information Process V1.0	No exceptions noted.
CC4.2.4	The Entity's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Inspected the Internal Audit Assessment report confirming review and approval. April 2025- MRM Minutes	No exceptions noted.
CC5.0: CONTROL ACTIVITIES			
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	Entity has developed a set of policies that establish expected behavior about the Company's control environment.	Inspected the environmental control policies. Frappe Business Code of Conduct V4.0	No exceptions noted.
CC5.1.2	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Observed assigned responsibilities and duties. ISMS Roles & Responsibilities	No exceptions noted.
CC5.1.3	Entity has a documented Acceptable Usage Policy, and makes it available for all staff on the company intranet	Inspected the Acceptable Usage Policy on the intranet. Acceptable Usage of Assets V.4.0	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	Entity's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.2	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies confirming review and approval. Frappe Control of Documented Information Process V1.0	No exceptions noted.
CC5.2.3	The Entity's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC5.2.4	Entity's Senior Management reviews and approves the Organizational Chart annually.	Inspected the Organizational Chart review records. Organization Chart V.4.0	No exceptions noted.
CC5.2.5	The Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report confirming review and approval. Approval Record	No exceptions noted.
CC5.2.6	Entity's InfoSec officer reviews and approves the list of people with access to production consoles annually.	Inspected the production console access list. Access Matrix – Role Based Permission Matrix	No exceptions noted.
CC5.2.7	The Entity's Senior Management reviews and approves the "supplier Risk Assessment Report" annually.	Inspected the Supplier Risk Assessment Report confirming review and approval. Approval Record	No exceptions noted.
CC5.2.8	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Observed subservice organization review records. April 2025- MRM Minutes	No exceptions noted.
CC5.2.9	Entity has developed a set of policies that set up expected behavior regarding the Company's control environment.	Inspected the environmental control policies. Frappe Business Code of Conduct V4.0	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3: COSO Principle 12: The entity deploys control activities through policies that set up what is expected and in procedures that put policies into action.			
CC5.3.1	Entity makes all policies and procedures available to all staff members via the company intra-net.	Inspected the company policies and procedures on the intranet. Document Published on the Spaces – Gameplan Evidence	No exceptions noted.
CC5.3.2	Entity requires that all staff members review and acknowledge company policies annually	Inspected acknowledgment records. New Policies will be available as newsletters for the employee to acknowledge. Evidence	No exceptions noted.
CC5.3.3	Entity requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to follow them.	Observed onboarding process and acknowledgment records. Employee Acknowledgment – Code of Conduct	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that set up expected behavior regarding the Company's control environment.	Inspected policies related to the control of the environment. Frappe Business Code of Conduct V4.0	No exceptions noted.
CC6.0: LOGICAL AND PHYSICAL ACCESS CONTROLS			
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 aims.			
CC6.1.1	Entity has developed an access control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	Inspected the access control policy. Access Control Process V.4.0	No exceptions noted.
CC6.1.2	Entity keeps a matrix that outlines which system components should be accessible to staff members based on their role.	Inspected the staff access matrix. Access Matrix – Role Based Permission Matrix	No exceptions noted.
CC6.1.3	Entity uses a continuous monitoring system, to alert the	Inspected the monitoring tool.	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	security team to update the access levels of team members whose roles have changed	The ERP System disables the ID, and all access will be removed.	
CC6.1.4	The Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to the entity's system.	Observed system access review by Senior Management or Information Security Officer.	No exceptions noted.
CC6.1.5	Entity's Senior Management or the Information Security Officer periodically reviews and approves the list of people with administrative access to the entity's system.	Observed administrative system access review.	No exceptions noted.
CC6.1.6	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access	Inspected access provisioning logs and approval by Information Security Officer.	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	Entity has developed an access control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	Inspected the control access policy. Access Control Process V.4.0	No exceptions noted.
CC6.2.2	Entity keeps a matrix that outlines which system components should be accessible to staff members based on their role.	Observed the staff access matrix. Access Matrix – Role Based Permission Matrix	No exceptions noted.
CC6.2.3	Staff access to the Entity's systems are made inaccessible on time as a part of the off-boarding process.	Observed the offboarding process.	No exceptions noted.
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information as-sets 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	Entity keeps a matrix that outlines which system components should be accessible to staff members based on their role.	Inspected the staff access matrix. Access Matrix – Role Based Permission Matrix	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.2	Staff access to Entity's systems are made inaccessible on time as a part of the off boarding process.	Inspected the offboarding process.	No exceptions noted.
CC6.3.3	Entity ensures that access to the infrastructure provider's environment (production console) is restricted to only those individuals who require such access to perform them job functions.	Inspected infrastructure access.	No exceptions noted.
CC6.3.4	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inspected production database access.	No exceptions noted.
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorize personnel to meet the entity's aims.			
Cc6.4.1	Entity relies on an infrastructure provider for hosting the systems supporting its production environment. As a result, there is no physical access available to its staff members.	Inspected production environment hosting arrangements. Cloud Security Management Process Vendor Management Process	No exceptions noted.
CC6.5: The entity drops 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	Entity provides guidance on decommissioning of information assets that have classified information in the Media disposal policy.	Inspected the Media Disposal Policy. Media Management Process V1.0	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	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor authentication	Inspected multifactor authentication mechanisms. Password Management Process PRO023 V4.0	No exceptions noted.
CC6.6.2	Entity requires that all endpoints with access to production systems are protected by malware-protection software.	Inspected malware protection software. Antivirus Management Process	No exceptions noted.
CC6.6.3	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access. Entity requires that all	Inspected encryption process.	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	critical endpoints are encrypted to protect them from unauthorized access	Frappe Endpoint Security Process	
CC6.6.4	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Inspected quarterly audit report on OS versions. Patch Management Process	No exceptions noted.
CC6.6.5	Entity requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity.	Inspected auto-screen-lock settings.	No exceptions noted.
CC6.6.6	Every Production host is protected by a security system with a deny-by- default rule. Deny by default rule set is a default on the Entity's cloud provider.	Security system settings inspected. Network Security Management Process	No exceptions noted.
CC6.6.7	Entity has a documented Endpoint Security Policy, and makes it available for all staff on the company intranet	Inspected Endpoint Security Policy availability. Frappe Endpoint Security Process	No exceptions noted.
CC6.6.8	Entity has a documented Password Policy and makes it available to all staff members on the company intranet	Password Policy availability. Password Management Process PRO023 V4.0	No exceptions noted.
CC6.6.9	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access	Observed access controls.	No exceptions noted.
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 aims.			
CC6.7.1	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access/ Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Observed encryption process and records. Cryptography & Key Management Process PRO021 V4.0	No exceptions noted.
CC6.7.3	All production databases[s] that store customer data are encrypted at rest.	Inspected encryption processes. Cryptography & Key Management Process PRO021 V4.0	No exceptions noted.
CC6.7.4	User access to the entity's application is secured using https	Inspected HTTPS (TLS encryption).	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	(TLS algorithm) and industry standard encryption.		
CC6.7.5	Entity keeps a list of production infrastructure assets and segregates production assets from its staging/development assets.	Inspected infrastructure segregation records. Asset List	No exceptions noted.
CC6.7.6	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment	Inspected protection measures for non-production environments.	No exceptions noted.
CC6.7.7	Entity has a documented Encryption Policy, and makes it available for all staff on the company intra-net	Encryption Procedure availability. Cryptography & Key Management Process PRO021 V4.0	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 aims.			
CC6.8.1	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Inspected OS version audit records.	No exceptions noted.
CC6.8.2	Every Production host is protect-ed by a security system with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Inspected security system settings on the cloud provider.	No exceptions noted.
CC7.0: SYSTEM OPERATIONS			
CC7.1: To meet its aims, 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	Entity finds vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected the vulnerability scan records. Evidence - VAPT Assessment Report	No exceptions noted.
CC7.1.2	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management process. Evidence – Procedure	No exceptions noted.
CC7.1.3	Entity's infrastructure is configured to generate audit events for actions of interest related to security, which are reviewed and analyzed for anomalies.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	Entity's production assets are continuously checked to generate alerts and take immediate action where necessary.	Inspected the Production assets and their alerting system.	No exceptions noted.
CC7.2: The entity checks 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	Entity finds vulnerabilities on the company platform through regular vulnerability scans.	Inspected the vulnerability scan records. Evidence - VAPT Assessment Report	No exceptions noted.
CC7.2.2	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management process. Evidence – Procedure	No exceptions noted.
CC7.2.3	Entity's infrastructure generates audit events for security-related actions, which are reviewed for anomalies.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC7.2.4	Entity's production assets are continuously checked to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.
CC7.3: The entity evaluates security events to decide 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	Entity uses a continuous monitoring system to track and report the health of the information security program to stakeholders.	Inspected the monitoring system and reporting.	No exceptions noted.
CC7.3.2	Entity requires all employee endpoints to be audited quarterly to ensure OS versions are current.	Inspected OS versions. Found to be up to date.	No exceptions noted.
CC7.3.3	Entity keeps a record of information security incidents.	Incident Report available and verified. Incident Report	No exceptions noted.
CC7.3.4	Entity finds vulnerabilities on the company platform through regular vulnerability scans.	Inspected the vulnerability scan records. Evidence - VAPT Assessment Report	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.5	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management process. Evidence – Procedure	No exceptions noted.
CC7.3.6	Entity finds vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.	Inspected the penetration testing exercise. Evidence - VAPT Assessment Report	No exceptions noted.
CC7.3.7	Entity's infrastructure is configured to generate audit events for security-related actions, which are reviewed for anomalies.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC7.3.8	Entity's production assets are continuously checked to generate alerts and take immediate action where necessary.	Inspected the Production assets and their alerting system. Procedure verified - Logging & Monitoring Process	No exceptions noted.
CC7.4: The entity responds to found security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The entity’s Information Security Officer performs an annual internal audit to assess and check the health of internal controls and shares findings in an "Internal Audit Assessment" report with Senior Management.	Inspected the internal audit assessment report. It has been reviewed and approved by Senior Management. Internal Audit Checklist	No exceptions noted.
CC7.4.2	Entity has an Incident Management & Response Policy with guidelines and procedures for responding to security incidents. The policy is available to all staff via the company intranet.	Inspected the procedure and availability on the intranet. Information Security Incident Management Process PRO025 V4.0	No exceptions noted.
CC7.4.3	Entity keeps a record of information security incidents.	Incident Report available and verified. Incident Report	Not Tested
CC7.5: The entity finds, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The Entity has documented Business Continuity & Disaster Recovery Policies that set up	Inspected the policies.	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	procedures for continuing business operations in case of disruption or security incident.	Business Continuity Management Process	
CC7.5.2	Entity has a documented Data Backup Policy and makes it available for all staff on the company intranet.	Inspected the policy and availability on the intranet. Backup & Restoration Process	No exceptions noted.
CC8.0: CHANGE MANAGEMENT			
CC8.1: The entity authorizes, designs, develops, or buys, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Entity has a documentation Change Management Policy, which is available to all Staff Members via the company intranet.	Inspected the Process and availability on the intranet. Change Management Process	No exceptions noted.
CC8.1.2	Entity uses a change management system to track, review, and log all changes to the application code through Bit-Bucket.	Inspected the management system. Change Management Process Asset Change Request	No exceptions noted.
CC8.1.3	Entity keeps a list of infrastructure assets and segregates production assets from staging/development assets.	Inspected the production infrastructure asset records. Asset List	No exceptions noted.
CC8.1.4	Entity's change management system enforces peer reviews for all planned changes. For code changes, the reviewer must be different from the author.	Inspected the management system. Change Management Process	No exceptions noted.
CC9.0: RISK MITIGATION			
CC9.1: The entity finds, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The entity has a documented Risk Assessment and Management Policy describing processes to find risks to business objectives and how they are assessed and mitigated.	Inspected the policy. Risk Assessment & Treatment Methodology	No exceptions noted.
CC9.1.2	Entity performs a formal risk assessment annually, as detailed in the Risk Assessment and Management Policy, to find threats that could impair system security commitments and requirements.	Inspected the policy and risk assessment records. Risk Assessment	No exceptions noted.

ss	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all risk.	Inspected the risk scoring and mitigation measures. Risk Assessment Risk Assessment & Treatment Methodology	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to find risks to business objectives and how those risks are assessed and mitigated. The aims incorporate Entity's service commitments and system requirements.	Inspected the policy. Risk Assessment Risk Assessment & Treatment Methodology	No exceptions noted.
CC9.2.2	Entity has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.	Inspected the procedure on Vendor Risk management. Vendor Risk Management Process	No exceptions noted.
CC9.2.3	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to find vendors that are critical to the system's security commitments and requirements	Inspected the policy and vendor risk assessment records. Risk Assessment Risk Assessment & Treatment Methodology	No exceptions noted.

Availability Principle and Criteria Table

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Evaluate Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
A.1.1: The entity keeps, 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	Entity Production assets are continuously checked to generate alerts and take immediate action where necessary.	Inspected the entity's production assets and their alerting system.	No exceptions noted.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Entity has documented physical and environmental controls and makes it available for all staff on the company intranet.	Inspected the Admin Procedure. Admin Procedure V.4.0	No exceptions noted.
A1.2.2	Entity backs-up their production databases periodically.	Inspected the periodical production database backups. Evidence	No exceptions noted.
A1.2.3	Entity data backups are restored and evaluated annually	Inspected the annual restoration and testing of data backups. Evidence	No exceptions noted.
A1.2.4	Entity has documented Business Continuity & Disaster Recovery Policies that set up guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity & Disaster Recovery Policies. Business Continuity Management Process	No exceptions noted.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its aims.			
A1.3.1	Entity has documented Business Continuity & Disaster Recovery Policies, which set up guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity & Disaster Recovery Policies. Business Continuity Management Process	No exceptions noted.
A1.3.2	Entity ensures that the Disaster Recovery Plan is evaluated periodically, and learnings documented	Inspected test of the Disaster Recovery Plan. Business Continuity Management Process	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Evaluate Results
		BCP Evidence	
A1.3.3	Entity data backups are restored and evaluated annually	Inspected the annual restoration and testing of data backups. Evidence	No exceptions noted.

Confidentiality Principle and Criteria Table

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Evaluate Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity finds and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Entity has a documentation Confidentiality Policy and makes it available for all staff on the company intranet.	Newsletter issued to all employees for communication and acknowledgment. It has been made available for all staff on the company intranet. Policy Communication Evidence	No exceptions noted.
C1.1.2	Entity requires that all new staff acknowledge the entity's confidentiality policy as part of their onboarding.	Inspected the NDA document. has been acknowledged by all new staff members. NDA - Evidence	No exceptions noted.
C1.1.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the Policies. It has been acknowledged by all staff members annually. Employee Acknowledgment – Code of Conduct	No exceptions noted.
C1.1.4	The entity has a documented Data Classification Policy and makes it available for all staff on the company intranet.	Inspected the Information Classification & Labelling Process. It has been made available for all staff on the company intranet. Information Classification & Labelling Process	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Evaluate Results
C1.1.5	All production databases[s] that store customer data are encrypted at rest.	Inspected the encryption process in the system. Verified procedure - Cryptography & Key Management Process	No exceptions noted.
C1.1.6	Entity requires that all company- owned endpoints be encrypted to protect them from unauthorized access	Inspected the encryption process in the system. Verified procedure - Cryptography & Key Management Process	No exceptions noted.
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Entity has a documented Data Retention Policy and makes it available for all staff on the company intranet.	The process on Control of documented information has been acknowledged by all new staff members. Frappe Control of Documented Information Process V1.0	No exceptions noted.
C1.2.2	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.	IT Media Management Process verified and found evident Media Management Process V1.0	No exceptions noted.

End of Report