SOC 2 TYPE 2 REPORT

Walkover Web Solutions Private Limited

MSG91

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2 TYPE 2 REPORT
ON MANAGEMENT'S DESCRIPTION

OF ITS

MSG91 SOFTWARE APPLICATION

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and
Test of Operating Effectiveness Relevant to Security, Availability, Confidentiality

For the Observation period : 26th January 2024 - 26th April 2024
Next Report Issue Date: 27th April 2025

TOGETHER WITH INDEPENDENT SERVICE AUDITORS' REPORT

You may use the SOC for Service Organisations logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organisations - Logo.

The next report would be issued on 27th April 2025 Subject to observation and examination by Atom Assurances

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To : Walkover Web Solutions Private Limited.

Scope

We have examined the accompanying "Description of Walkover Web Solutions Private Limited, MSG91 Software Application. "
Throughout the period "26th January 2024 - 26th April 2024", and the suitability of the design and operating effectiveness of controls to meet Walkover Web Solutions Private Limited service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity & Privacy principles set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality and Availability (applicable trust services criteria) throughout the period 26th January 2024 - 26th April 2024.

Walkover Web Solutions Private Limited uses,
- Amazon Web services(AWS), a subservice organization which provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis via Software-As-A-Service (SaaS).
- Github(Github Inc), is a platform and cloud-based service for software development and version control using Git, allowing developers to store and manage their code.
- MongoDB is a source-available, cross-platform, document-oriented database program. Classified as a NoSQL database product, MongoDB utilizes JSON-like documents with optional schemas. MongoDB is developed by MongoDB Inc. and current versions are licensed under the Server Side Public License (SSPL).
- MySQL is a widely used relational database management system (RDBMS). MySQL is free and open-source. MySQL is ideal for both small and large applications.
- Google LLC (Google Workspace), a collection of cloud computing, productivity and collaboration tools, software, and products such as E-mail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more.

The description presents Walkover Web Solutions Private Limited controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Walkover Web Solutions Private Limited controls.

The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description presents Walkover Web Solutions Private Limited controls, the applicable trust services criteria and the types of complementary user entity controls assumed in the design of Walkover Web Solutions Private Limited 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 subservice organization controls.

Service Organization's Responsibilities

Walkover Web Solutions Private Limited has provided the accompanying assertion titled " Walkover Web Solutions Private Limited Management Assertion throughout the period 26th January 2024 - 26th April 2024." about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet Walkover Web Solutions Private Limited service commitments and system requirements based on the applicable trust services criteria.

Walkover Web Solutions Private Limited is responsible for:
1. Preparing the description and assertion;
2. The completeness, accuracy and method of presentation of the description and assertion;
3. Providing the services covered by the description;
4. Identifying the risks that would prevent the applicable trust services criteria from being met;
5. Designing, implementing, maintaining and documenting controls to meet Walkover Web Solutions Private Limited service commitments and system requirements based on the applicable trust services criteria stated in the description.
6. Specifying the controls that meet Walkover Web Solutions Private Limited service commitments and system requirements based on the applicable trust services criteria and stating them 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 Walkover Web Solutions Private Limited assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organizations commitments and system requirements were met based on applicable trust services criteria.

We conducted our examination in accordance with 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 the service organization's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria

3. The controls operated effectively to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 26th January 2024 - 26th April 2024.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's commitments and system requirements meet the applicable trust services criteria.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the service organization's commitments and system requirements based on the applicable trust services criteria were met. Our examination also included evaluating 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 each individual user may consider important to its own particular 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.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks 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 tested and the nature and timing, and results of those tests are listed in the accompanying description of Criteria, Controls, Tests and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria described in Walkover Web Solutions Private Limited assertion and the applicable trust services criteria:

1. The description fairly presents the MSG91 Software Application by Walkover Web Solutions Private Limited that was designed and implemented throughout the period "26th January 2024 - 26th April 2024".

2. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities applied the controls contemplated in the design of Walkover Web Solutions Private Limited controls throughout the period 26th January 2024 - 26th April 2024.

3. The controls tested, which were those necessary to provide reasonable assurance that the service organizations commitments and system requirements based on the applicable trust services principles criteria were met, operated effectively throughout the period "26th January 2024 - 26th April 2024".

Restricted Use

This report, including the description of tests of controls and results thereof in the description of tests and results is intended solely throughout information and use of user entities of Walkover Web Solutions Private Limited throughout the period 26th January 2024 - 26th April 2024., and prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of service provided by the service organization.
- How the service organizations' system interacts with the user entities, subservice organizations, or other parties.
- Internal controls and its limitations.
- Complementary subservice organizations and complementary user entity controls and how those controls interact with the controls at the service organizations to achieve the service organization's 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 controls address those risks.

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

MISHRA

Neha Mishra, Certified Public Accountant

License No.: PAC-CPAP-LIC-033276

Date: 15th May 2024

SECTION 2

MANAGEMENT's ASSERTION

MANAGEMENT'S ASSERTION

Walkover Web Solutions Private Limited Management Assertion for the Period
"26th January 2024 - 26th April 2024".

We have prepared the attached description titled "Description of Walkover Web Solutions Private Limited - MSG91 Software Application" for the period "26th January 2024 - 26th April 2024", based on the criteria for a description of a service organization's system in DC section 200 prepared by AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group to be used in conjunction with the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (the description criteria). The description is intended to provide users with information about the MSG91 Software Application provided by Walkover Web Solutions Private Limited, that may be useful when assessing the risks from interactions with the system throughout the period 26th January 2024 - 26th April 2024. particularly information about the suitability of the design and operating effectiveness of controls to meet Walkover Web Solutions Private Limited service commitments and system requirements based on the criteria related to Security, Confidentiality & Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy, (AICPA, Trust Services Criteria).*

Walkover Web Solutions Private Limited uses,
- Amazon Web services(AWS), a subservice organization which provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis via Software-As-A-Service (SaaS).
- Github(Github Inc), is a platform and cloud-based service for software development and version control using Git, allowing developers to store and manage their code.
- MongoDB is a source-available, cross-platform, document-oriented database program. Classified as a NoSQL database product, MongoDB utilizes JSON-like documents with optional schemas. MongoDB is developed by MongoDB Inc. and current versions are licensed under the Server Side Public License (SSPL).
- MySQL is a widely used relational database management system (RDBMS). MySQL is free and open-source. MySQL is ideal for both small and large applications.
- Google LLC (Google Workspace), a collection of cloud computing, productivity and collaboration tools, software, and products such as E-mail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more.

The description presents Walkover Web Solutions Private Limited controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Walkover Web Solutions Private Limited controls.

The description indicates that complementary user entity organization controls that are suitably designed and operating effectively are necessary, along with controls at Walkover Web Solutions Private Limited. to achieve Walkover Web Solutions Private Limited. 's service commitments and system requirements based on the applicable trust services criteria. The description presents Walkover Web Solutions Private Limited controls, the applicable trust services criteria and the types of complementary user entity organization controls assumed in the design of Walkover Web Solutions Private Limited controls. The description does not disclose the actual controls at the user entity organizations.

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

1. The description fairly presents the MSG91 Software Application provided by Walkover Web Solutions Private Limited. throughout the period 26th January 2024 - 26th April 2024. The criteria for description are identified below under the heading "Description Criteria".

2. The controls stated in the description were suitably designed and operated effectively to meet Walkover Web Solutions Private Limited service commitments and system requirements based on the applicable trust services criteria throughout the period 26th January 2024 - 26th April 2024., to meet the applicable trust services criteria.

Description Criteria:
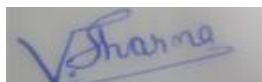
The description contains the following information:

- The types of services provided.
- The principal 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 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.

For Walkover Web Solutions Private Limited

Authorized Signatory

SECTION 3- System Description

Walkover Web Solutions Private Limited description of its MSG91 Software Application

MSG91 is a cloud-hosted software application built by Walkover Web Solutions hereby referred to as Walkover Web Solutions.

MSG91 is empowering developers with communication APIs in addition to building tools & supporting ideas that run majorly on communication.

Any other services provided by Walkover Web Solutions are not in the scope of this report

Principal Service Commitments and System Requirements

Walkover Web Solutions designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Walkover Web Solutions makes to customers and the compliance requirements that Walkover Web Solutions has established for their services.

Security commitments to user entities are documented and communicated in Walkover Web Solutions's customer agreements, as well as in the description of the service offering provided online. Walkover Web Solutions's security commitments are standardized and based on some common principle

Security commitments include, but are not Limited to, the following:

- The fundamental design of Walkover Web Solutions's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role
- Walkover Web Solutions implements various procedures and processes to control access to the production environment and the supporting infrastructure
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics

Confidentiality commitments include, but are not Limited to, the following:
- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Walkover Web Solutions and user entities.

Availability commitments include, but are not Limited to, the following:
- System performance and availability monitoring mechanisms to help ensure the consistent delivery of
- the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans are tested on a periodic basis; and,
- Operational procedures supporting the achievement of availability commitments to user entities

Walkover Web Solutions establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Walkover Web Solutions's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how staff is hired.

Components of the System used to provide services

Infrastructure & Network Architecture

The production infrastructure for the MSG91 software application is hosted on AWS in their various regions across Singapore, India, Ireland.

MSG91 Software Application uses a virtual and secure network environment on top of AWS infrastructure to ensure that theMSG91 Software Application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. MSG91 Software Application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the AWS, Internet Gateway, over to a Virtual Private Cloud that

1. Houses the entire application runtime
2. Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that
only deliberately allowed traffic can pass through.

NETWORK ARCHITECTURE DIAGRAM
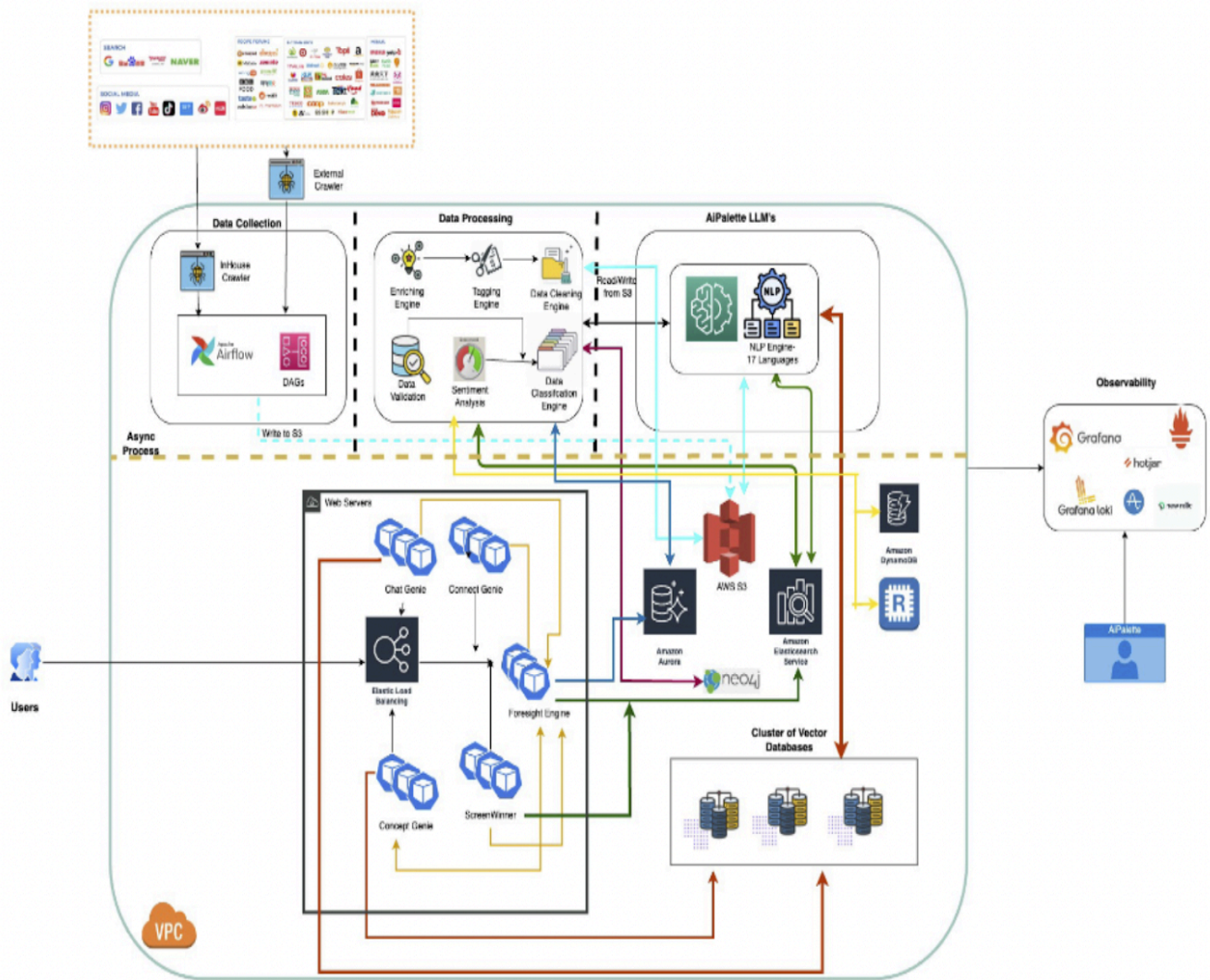
Software

Walkover Web is responsible for managing the development and operation of the Walkover Web platform including infrastructure components such as servers, databases, and storage systems.

The in-scope Walkover Web infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**OS DB**	**Physical Location**
MSG91 Software Application	Access to the MSG91 SaaSapplication is through a web/mobile interface and user authentication.	MYSQL & MongoDB	AWS Singapore, India, Ireland
AWS IAM	Identity and access management console	Amazon Proprietary	AWS
AWS Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic	Amazon Proprietary	AWS
Github	Source code repository, version control system, and build software.	Github Proprietary	Github Cloud
Google workspace	Identity/Email provider for all Walkover Web employees	Google Proprietary	Google LLC

Supporting Tools	
System /Application	**Business Function / Description**
PHP,Python,Angular	Programming Language used for MSG91 Software Application
Sprinto	Provide continuous compliance monitoring of the company's system.
Google Workspace	Office communication services

People

Walkover Web Solutions's staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel has also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training

Procedures and Policies

Formal policies and procedures have been established to support the Walkover Web application.

These policies cover:
- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Walkover Web also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the MSG91 Software Application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

Data, as defined by Walkover Web, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Output reports are available and include data and files systematically generated from the system. The availability of these reports is Limited by job function. Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed, and stored as a part of the MSG91 Software Application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is Limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally, or was entrusted to Walkover Web Solutions Private Limited by others.Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Walkover Web Solutions Private Limited PII • Unpublished financial information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies

Data Sensitivity	Description	Examples
Internal	Information if it went outside the Walkover Web and could impact performance or result in low levels of financial loss to Walkover Web. The information, artifacts, policy documents, etc. marked as internal can be shared with the employees internally. Information if it went outside the Walkover Web and could impact performance or result in low levels of financial loss to Walkover Web.	• Policies • Internal documents
Public	Information that could be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to the corporation.	• Website • Information available on websites, blogs, etc. • Press releases

Customer data is retained per the regulatory requirements and the agreements with customers and will be disposed of upon request by customers. A confirmation will be sent back to the customer to notify them that the disposal is complete.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS are responsible for the physical security controls of the in-scope system. Walkover Web reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the MSG91 Software Application.

Incident Management

Walkover Web has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Walkover Web via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there are problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low-severity incidents** are those that do not require immediate remediation. These typically include a partial service of Walkover Web being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
- **High-severity incidents** are problems with an active security attack that has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application 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 private cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include but are not Limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by Walkover Web management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

Walkover Web only uses network ports, protocols, and services listening on a system with validated business needs to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to Walkover Web's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Walkover Web 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

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Walkover Web are reviewed, deployed, and managed. The policy covers all changes made to the MSG91 Software Application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted MSG91 Software Application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the MSG91 Software Application can be initiated by a staff member with an appropriate role. Walkover Web uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Customer content and personal information are not used in non-production environments.

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. Walkover Web uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management, and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

External penetration tests are performed at least annually and include a full scope of blended attacks, such as client-based and web application attacks.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include 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

Walkover Web 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.

Boundaries of the System

The scope of this report includes the MSG91 software application. It also includes the people, processes, and IT systems that are required to achieve our service commitments toward the customers of this application. Walkover Web Solutions depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

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

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Walkover Web's description of the system.

This section provides information about the five interrelated components of internal control at Walkover Web Solutions Private Limited including:
- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

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 monitor them. Integrity and ethical values are essential elements of Walkover Web's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Walkover Web's 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.

Walkover Web and its management team have established the following controls to incorporate ethical values throughout the organization:
- A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members
- Staff members are required to 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

Walkover Web's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- 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 the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining 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

Walkover Web's 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 interaction with independent assessments of the company's operations and information security posture.

Management Philosophy and Operating Style

Walkover Web's 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. Walkover Web's control environment reflects the philosophy of management. Walkover Web's information security function, composed of senior management and the Information Security Officer, meets frequently 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 Walkover Web has implemented in this area are described below:

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

Human Resources

Walkover Web's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating 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 are required to 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 deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

Risk Assessment

Walkover Web regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Walkover Web's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. Walkover Web identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the MSG91 Software Application, and management has implemented various measures designed to manage these risks.

Walkover Web believes that effective risk management is based on the following principles:
Senior management's commitment to the security of MSG91 Software Application

- The involvement, cooperation, and insight of all Walkover Web staff
- Initiating risk assessments with discovery and identification of risks
- Thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all Walkover Web staff to report risks and threat vectors

Scope

The risk assessment and management program applies to all systems and data that are a part of the MSG91 Software Application. The Walkover Web risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Walkover Web's Information Security Officer and the department or individuals responsible for the area being assessed. All Walkover Web staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment
Walkover Web uses a number of vendors to meet its business objectives. Walkover Web understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Walkover Web employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Walkover Web assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Walkover Web's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment.

Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment
As part of the design and operation of the system, Walkover Web identifies the specific risks that service commitments may not be met and designs controls necessary to address those risks. Walkover Web's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Control Activities

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

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

Logical Access Control

The MSG91 Software Application 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 MSG91 Software Application and authenticates to the database.

Walkover Web has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform 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 within three business days.

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

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Walkover Web customer data. Staff are encouraged to use passwords that 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 requires multi-factor authentication (MFA). Additionally, company-owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Information and Communication

Walkover Web 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, Walkover Web 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

Walkover Web's management monitors controls 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 are 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 between 26th January 2024 - 26th April 2024 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

Walkover Web'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 service criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing transactions for Walkover Web customers.

For customers to rely on the information processed through Walkover Web's MSG91 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.

The User entity is responsible for managing their organization's MSG91 Software Application account as well as establishing any customized security solutions or automated processes through the use of setup featuresThe User entity is responsible for protecting established user IDs and passwords within their organizations.

The User entity is responsible for reviewing customer access to Walkover Web'sMSG91 Software Application periodically to validate the appropriateness of access levels.

- The user entity is responsible for approving and creating new user access to Walkover Web's MSG91 Software Application.
- The user entity is responsible for removing terminated employee access to Walkover Web's MSG91 Software Application.
- The user entity is responsible for implementing policies and procedures regarding the types of data that are allowed to be entered into Walkover Web's MSG91 Software Application.
- The user entity is responsible for sending data to Walkover Web's MSG91 Software Application via a secure connection and/or the data should be encrypted.
- The user entity is responsible for notifying Walkover Web's MSG91 Software Application if they detect or suspect a security incident related to the Walkover Web.
- User entity is responsible for reviewing email and other forms of communications from Walkover Web, related to changes that may affect Walkover Web customers and users, and their security or availability obligations.
- The user entity is responsible for establishing, monitoring, and maintaining controls over the security of system-generated outputs and reports from the system.
- The user entity is responsible for endpoint protection of workstations used to access the system.
- The user entity is responsible for developing its own business continuity and disaster recovery plan.

Complementary Subservice Organization Controls

Walkover Web uses sub-service organizations in support of its system. Walkover Web'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 Walkover Web to be achieved solely by Walkover Web. Therefore, user entity controls must be evaluated in conjunction with Walkover Web's controls described 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.

Walkover Web periodically reviews the quality of the outsourced operations by various methods including:

- Review of sub-service organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS	CC6.1, 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 tested 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 Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	AWS	C1.1
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	AWS	C1.2

SECTION 4- Test Control Matrix

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the MSG91 Software Application provided by Walkover Web Solutions Private Limited.The scope of the testing was restricted to Walkover Web Solutions Private Limited, and its boundaries as defined in Section 3.

Walkover Web Solutions Private Limited conducted the examination testing for the observation period "26th January 2024 - 26th April 2024"

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, Walkover Web Solutions Private Limited. 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 mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the 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	Inquired of 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, or a 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, approval, 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, Atom Assurances 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. Atom Assurances, 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 aforementioned, 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.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	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 Business Conduct and makes it available to all staff members on the company intranet.	Inspected the Code of Business conduct. Available on the company intranet.	No exceptions noted.
CC1.1.2	Entity requires that new employees review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	Inspected the Code of Business conduct. Has been reviewed and acknowledged by staff members annually.	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.	No exceptions noted.
CC1.2.2	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the MRM minutes. The Information Security program has been reviewed and approved by the Senior Management.	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 approved by Senior Management.	No exceptions noted.
CC1.2.4	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC1.2.5	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	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 exceptions noted.
CC1.3.2	Entity ensures clarity in job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organization	Inspected the job descriptions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.	No exceptions noted.
CC1.4.2	Entity ensures that new hires go through a background check as part of their onboarding process.	Observed the onboarding background check for new hires.	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 Information. Contents are available for all staff on the company intranet.	No exceptions noted.
CC1.5.2	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.	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 responsibilities.	Observed the periodical evaluation of job responsibilities.	No exceptions noted.
CC1.5.4	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been reviewed and acknowledged by staff members.	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 functioning of internal controls. Has been reviewed and evaluated in the system.	No exceptions noted.
CC2.1.2	Entity makes all policies and procedures available to all staff members via the company intranet.	Inspected the policies and procedures. Has been made available to all staff members via the company intranet.	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 their website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 Business Conduct and makes it available to all staff members on the company intranet.	Inspected the behavioral standards which are defined in the Code of Business Conduct. Has been made available to all staff members on the company intranet.	No exceptions noted.
CC2.2.2	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 annual Security Awareness training records.	No exceptions noted.
CC2.2.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the company policies. Has been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.4	Entity makes all policies and procedures available to all staff members via the company intranet.	Inspected the policies and procedures have been made available to all staff members on the company intranet.	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.	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 comply with them.	Inspected the company policies have been reviewed and acknowledged by the new staff members.	No exceptions noted.
CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	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 its website.	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.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.0: RISK ASSESSMENT			
CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Entity has formally documented policies and procedures to govern risk management.	Inspected the risk management policies and procedures.	No exceptions noted.
CC3.1.2	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.
CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	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 of the risk.	Observed the risk mitigating factors.	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 comply with them.	Inspected if the company policies have been reviewed and acknowledged by the new staff members.	No exceptions noted.
CC3.2.4	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
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.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records. Inspected Assessment and Management Policy.	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 of the risk.	Observed the risk mitigating factors.	No exceptions noted.
CC3.4.3	Entity performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements.	Observed the annual formal risk assessment exercise records.	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.	Inspected the planning, assessing, implementing and internal control environment.	No exceptions noted.
CC4.1.2	Entity appoints an owner of Infrastructure, who is responsible for all assets in the inventory.	Inspected Infra Operations Person document. Said person is responsible for all assets in the inventory.	No exceptions noted.
CC4.1.3	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Sprinto tool that continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.1.4	Entity's Senior Management reviews and approves all company policies annually.	Inspected the annual company policy has been reviewed and approved by Senior Management.	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 to confirm that the Information Security program has been reviewed and approved by the Senior Management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.6	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 approved by Senior Management.	No exceptions noted.
CC4.1.7	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.1.8	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	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 organizations defined in the system. Has been reviewed and evaluated by the entity.	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 Information security policy.	No exceptions noted.
CC4.2.2	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the continuous monitoring system, Sprinto. Has been tracking and reporting the health of the information security program continually.	No exceptions noted.
CC4.2.3	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC4.2.4	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the MRM minutes. Information Security program has been reviewed and approved by the Senior Management.	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 with regard to the Company's control environment.	Inspected the control environment policies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 the responsibilities and duties across the organization.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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. Has been made available for all staff on the company intranet.	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 uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the continuous monitoring system, Sprinto. Has been tracking and reporting the health of the information security program continually.	No exceptions noted.
CC5.2.2	Entity's Senior Management reviews and approves all company policies annually.	Inspected the company policies. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.3	Entity's Senior Management reviews and approves the state of the Information Security program annually	Inspected the MRM minutes. Information Security program has been reviewed and approved by the Senior Management.	No exceptions noted.
CC5.2.4	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the employees Organizational Chart. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.5	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Assessment Report. Has been reviewed and approved by Senior Management.	No exceptions noted.
CC5.2.6	Entity's Infosec officer reviews and approves the list of people with access to production console annually.	Inspected the production console list in the system. Has been reviewed and approved by Infosec officer.	No exceptions noted.
CC5.2.7	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the Vendor Risk Assessment Report. Has been reviewed and approved by Senior Management.	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 the periodic reviews and evaluations of subservice organizations in the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.9	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the control environment policies.	No exceptions noted.
CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Entity makes all policies and procedures available to all staff members via the company intranet.	Inspected the company policies and procedures. Has been made available to all staff members via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.2	Entity requires that all staff members review and acknowledge company policies annually.	Inspected company policies. Has been reviewed and acknowledged by all staff members.	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 comply with them.	Observed the responsibilities of new staff members in the system. Has been reviewed and acknowledged by all staff members.	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Observed policies in the system relating to the control environment.	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 objectives.			
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.	No exceptions noted.
CC6.1.2	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Observed the staff access matrix.	No exceptions noted.
CC6.1.3	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.	Inspected the Sprinto tool that continuously monitors and alerts the security team to update the access levels of team members whose roles have changed.	No exceptions noted.

CC6.1.4	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions	Inspected user access review for critical systems in Sprinto compliance automation tool.	No exceptions noted.
CC6.1.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions	Inspected administrative access review for critical systems through Sprinto compliance automation tool.	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 entity's access provisioning logs. Has been reviewed and approved by the 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 access control policy.	No exceptions noted.
CC6.2.2	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Observed the staff access matrix.	No exceptions noted.
CC6.2.3	Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding 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 assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

CC6.3.1	Entity maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Observed the staff access matrix.	No exceptions noted.
CC6.3.2	Staff access to Entity's systems are made inaccessible in a timely manner as a part of the offboarding process.	Observed 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 their job functions.	Observed the access infrastructure.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.	Observed the 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 authorized personnel to meet the entity's objectives.			
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.	Observed the production environment hosted by the infrastructure provider.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.	Inspected the Media disposal policy.	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 Multi factor authentication.	Observed the Multifactor authentication for all critical system.	No exceptions noted.
CC6.6.2	Entity requires that all endpoints with access to production systems are protected by malware-protection software.	Observed the malware-protection software.	No exceptions noted.
CC6.6.3	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Observed the encryption process for unauthorized access.	No exceptions noted.
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 the quarterly audit report on the Operating System.	No exceptions noted.
CC6.6.5	Entity requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity.	Observed the auto-screen-lock process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.6	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the Entity's firewall in the system.	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 the Endpoint Security Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
CC6.6.8	Entity has a documented Password Policy and makes it available to all staff members on the company intranet.	Inspected the Password Policy. Has been made available for all staff on the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Observed that access to all entity-owned endpoints is encrypted.	No exceptions noted.
CC6.7.2	All production database[s] that store customer data are encrypted at rest.	Observed the encryption process.	No exceptions noted.
CC6.7.3	User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.	Observed the https (TLS algorithm) and industry standard encryption.	No exceptions noted.
CC6.7.4	Entity maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.	Observed the production infrastructure assets records. Has been segregated from staging/development assets.	No exceptions noted.
CC6.7.5	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Observed production and non-production environments maintain the same level of protection for customer data.	No exceptions noted.
CC6.7.6	Entity has a documented Encryption Policy and makes it available for all staff on the company intranet.	Inspected the Encryption Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Entity requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Observed the version on Operating System. Has been found to be up to date.	No exceptions noted.

CC6.8.2	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the Entity's cloud provider's firewall.	No exceptions noted.

CC7.0: SYSTEM OPERATIONS

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

CC7.1.1	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.1.2	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management Policy.	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 anomalous or suspicious activity.	Observed Threat detection system enabled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

CC7.2.1	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.2.2	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management Policy.	No exceptions noted.
CC7.2.3	Entity's infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.	Inspected the internal audit logs. Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program	No exceptions noted.
CC7.2.4	Entity's Production assets are continuously monitored 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 determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

CC7.3.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the continuous monitoring system, Sprinto. Has been tracking and reporting the health of the information security program continually.	No exceptions noted.
CC7.3.2	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 the quarterly audit report on Operating System.	No exceptions noted.
CC7.3.3	Entity maintains a record of information security incidents.	Inspected the record of information security incidents.	No exceptions noted.
CC7.3.4	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Observed the vulnerability scans records.	No exceptions noted.
CC7.3.5	Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third-party service provider.	Observed the annual penetration testing exercise	No exceptions noted.
CC7.3.6	Entity tracks all vulnerabilities and resolves them as per the Vulnerability Management Policy.	Inspected the Vulnerability Management Policy.	No exceptions noted.
CC7.3.7	Entity's infrastructure is configured to generate audit events for actions of interest related to security which are reviewed and analyzed for anomalous or suspicious activity.	Inspected the internal audit logs. Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program.	No exceptions noted.
CC7.3.8	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed the Production assets and their alerting system.	No exceptions noted.
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders	Inspected the continuous monitoring system, Sprinto. Has been tracking and reporting the health of the information security program continually.	No exceptions noted.
CC7.4.2	Entity has established an Incident Management & Response Policy, which includes guidelines and procedures to be undertaken in response to information security incidents. This is available to all staff members via the company intranet.	Inspected the Incident Management & Response Policy. Has been made available to all staff members via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Entity maintains a record of information security incidents.	Inspected the record of information security incidents.	No exceptions noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5.1	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity & Disaster Recovery Policies.	No exceptions noted.
CC7.5.2	Entity has a documented Data Backup Policy and makes it available for all staff on the company intranet.	Inspected the Data Backup Policy. Has been made available for all staff on the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.0: CHANGE MANAGEMENT			
CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Entity has a documented Change Management Policy, which is available to all Staff Members via the company intranet.	Inspected the Change Management Policy. Has been made available to all Staff Members via the company intranet.	No exceptions noted.
CC8.1.2	Entity uses a change management system to track, review and log all changes to the application code.	Observed the change management system.	No exceptions noted.
CC8.1.3	Entity maintains a list of infrastructure assets and segregates production assets from its staging/development assets.	Observed the production infrastructure assets records. Has been segregated from staging/development assets.	No exceptions noted.
CC8.1.4	Entity's change management system is configured to enforce peer reviews for all planned changes. For all code changes, the reviewer must be different from the author.	Observed the change management system.	No exceptions noted.
CC9.0: RISK MITIGATION			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Entity has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	Inspected the Risk Assessment and Management Policy. Observed the annual risk assessment exercise.	No exceptions noted.
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 of the risk.	Observed the risk score and mitigating factors.	No exceptions noted.
Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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 identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Assessment and Management Policy.	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 Vendor Management Policy.	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 identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Risk Assessment and Management Policy. Observed the annual vendor risk assessment exercise.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
A.1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Observed 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 a documented Data Backup Policy and makes it available for all staff on the company intranet.	Inspected the Data Backup Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
A1.2.2	Entity backs-up their production databases periodically.	Observed the periodical production databases backs-up.	No exceptions noted.
A1.2.3	Entity's data backups are restored and tested annually.	Observed the annual restoration and testing of data backups.	No exceptions noted.
A1.2.4	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity & Disaster Recovery Policies.	No exceptions noted.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity & Disaster Recovery Policies.	No exceptions noted.
A1.3.2	Entity ensures that the Disaster Recovery Plan is tested periodically, and learnings documented.	Observed test of the Disaster Recovery Plan.	No exceptions noted.
A1.3.3	Entity's data backups are restored and tested annually.	Observed the annual restoration and testing of data backups.	No exceptions noted.

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Entity has a documented Confidentiality Policy and makes it available for all staff on the company intranet.	Inspected the Confidentiality Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
C1.1.2	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 comply with them.	Inspected the Confidentiality Policy. Has been acknowledged by all new staff members.	No exceptions noted.
C1.1.3	Entity requires that all staff members review and acknowledge company policies annually.	Inspected the Policies. Has been acknowledged by all staff members annually.	No exceptions noted.
C1.1.4	Entity has a documented Data Classification Policy and makes it available for all staff on the company intranet.	Inspected the Data Classification Policy. Has been made available for all staff on the company intranet.	No exceptions noted.
C1.1.5	All production database[s] that store customer data are encrypted at rest.	Observed the encryption process in the system.	No exceptions noted.
C1.1.6	Entity requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Observed the encryption process in the system.	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.	Inspected the Data Retention Policy. Has been acknowledged by all new staff members.	No exceptions noted.
C1.2.2	Entity provides guidance on decommissioning of information assets that contain classified information in the Media disposal policy.	Inspected the Media disposal policy.	No exceptions noted.