System and Organization Controls (SOC) 2 Type I
Report on Management's Description of its

Vaultedge Mortgage Automation Software Application

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security, Availability, and Confidentiality

As of August 11, 2022

Together with
Independent Service Auditors' Report

Table of Contents

I. Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management of Vaultedge Software Private Limited (Vaultedge)

Scope

We have examined Vaultedge's accompanying description of its Vaultedge Mortgage Automation Software Application titled "Description of Vaultedge's Vaultedge Mortgage Automation Software Application" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of August 11, 2022, to provide reasonable assurance that Vaultedge's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Vaultedge is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Vaultedge's service commitments and system requirements were achieved. Vaultedge has provided the accompanying assertion titled "Assertion of Vaultedge Management" (assertion) about the description and the suitability of the design of controls stated therein. Vaultedge is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

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

Opinion

In our opinion, in all material respects,

a. The description presents Vaultedge's Vaultedge Mortgage Automation Software Application that was designed and implemented as of August 11, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of August 11, 2022, to provide reasonable assurance that Vaultedge service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of Vaultedge, user entities of Vaultedge's Vaultedge Mortgage Automation Software Application as of August 11, 2022, business partners of Vaultedge subject to risks arising from interactions with the Vaultedge Mortgage Automation Software Application, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

San Jose, California
September 15, 2022

II. Assertion of Vaultedge Management

Assertion of Vaultedge Management

We have prepared the accompanying description of Vaultedge's Vaultedge Mortgage Automation Software Application system titled *"Description of Vaultedge's Vaultedge Mortgage Automation Software Application*" as of August 11, 2022, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Vaultedge Mortgage Automation Software Application system that may be useful when assessing the risks arising from interactions with Vaultedge's system, particularly information about system controls that Vaultedge has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (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*).

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

a. The description presents Vaultedge's Vaultedge Mortgage Automation Software Application system that was designed and implemented as of August 11, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of August 11, 2022, to provide reasonable assurance that Vaultedge's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Signed by Vaultedge Management

September 15, 2022

III. Description of Vaultedge's Vaultedge Mortgage Automation Software Application

Description of Vaultedge's Vaultedge Mortgage Automation Software Application

Company Background

Vaultedge Mortgage Automation is a cloud-hosted software application built by Vaultedge Software Private Limited.

Services Provided

Vaultedge has created a cloud-hosted, software application to help mortgage lenders & servicers process more loans with less people. Vaultedge Mortgage Automation software automates the indexing of documents in a loan package and extracts the needed metadata from the loan package saving both time and cost. Vaultedge aims to make Mortgage Underwriting a real-time automated process resulting in massive savings in time and cost.

Any other services provided by Vaultedge are not in the scope of this report.

Principal Service Commitments and System Requirements

Vaultedge designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Vaultedge makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Vaultedge has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- The fundamental design of Vaultedge'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;
- Vaultedge 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;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

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 Vaultedge 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 that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in Vaultedge'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 business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

Infrastructure

The Vaultedge Mortgage Automation is hosted in Amazon Web Services (AWS) in their US-East-1, US-East-2,US-West-1,US-West-2 region and in Microsoft Azure US East region. Vaultedge Mortgage Automation software application uses a virtual and secure network environment on top of AWS infrastructure to ensure that the 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.

Vaultedge Mortgage Automation 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 an AWS Internet Gateway, over to a virtual private cloud that:

- Houses the entire application runtime

- Protects the application runtime from any external networks

The internal networks of AWS and Azure are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through. Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats.

Software

Vaultedge is responsible for managing the development and operation of the Vaultedge Mortgage Automation platform including infrastructure components such as servers, databases, and storage systems. The in-scope Vaultedge Mortgage Automation infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**OS DB**	**Physical Location**
Vaultedge Mortgage Automation - Main Web App	Vaultedge Mortgage Automation software automates the indexing of documents in a loan package and extracts the needed metadata from the loan package saving both time and cost. Access to the Vaultedge Mortgage Automation SaaS application is through a web interface and user authentication.	MongoDB	AWS US-West-1 AWS US-West-2 AWS US-East-1 AWS US-East-2
AWS and Azure IAM	Identity and access management console for AWS and Azure resources.	AWS/Azure Proprietary	AWS/Azure
AWS/Azure Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	AWS/Azure Proprietary	AWS/Azure

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**OS DB**	**Physical Location**
Bitbucket	Source code repository, version control system, and build software.	Bitbucket	Bitbucket Cloud
Amazon Simple Storage Services (S3)	Provides an interface used to store and retrieve business unit data. S3 APIs provide bucket- and object-level access and version control. S3 is controlled through the AWS IAM interface.	AWS Proprietary	AWS
GSuite	Identity/Email provider for all Vaultedge employees	Google Proprietary	GCP(Gmail)

Supporting Tools	
System / Application	**Business Function / Description**
AWS Elastic Beanstalk	Service for deploying and scaling web applications and services
AWS CloudTrail	Security event logging for AWS resources
AWS CloudWatch	Security and operational monitoring and event logging for AWS resources
AWS GuardDuty	Threat detection service that continuously monitors for malicious activity and unauthorized behavior for AWS resources
Slack	Office communication services

People

Vaultedge's staff have been organized into various functions like Sales, Support, Engineering, Product Management etc. The personnel have also been assigned 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 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, vulnerabilities, and adding controls to mitigate this risk. 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 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.

Data

Data, as defined by Vaultedge, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Loan files (related to mortgage)
- 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 Vaultedge Mortgage Automation 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 Vaultedge by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Vaultedge's 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
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public websites

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

Procedures and Policies

Formal policies and procedures have been established to support the Vaultedge Mortgage Automation software 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).

Vaultedge 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 (Vaultedge Mortgage Automation) software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Physical Security

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

Logical Access

The Vaultedge Mortgage Automation 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 software application and authenticates to the database.

Vaultedge 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 are 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 assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.

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

Computer Operations – Backups

Customer data is backed up by Vaultedge's operations team. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

Vaultedge 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.

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 Vaultedge are reviewed, deployed, and managed. The policy covers all changes made to the Vaultedge Mortgage Automation 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 software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Vaultedge Mortgage Automation software application can be initiated by a staff member with an appropriate role. Vaultedge 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 into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. Further AWS CloudTrail is configured to track all changes to the production infrastructure.

Data Communications

Vaultedge has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. Our PaaS simplifies our logical network configuration by providing an effective firewall around all the Vaultedge application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

Our PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Vaultedge engages an external security firm to perform quarterly vulnerability scans and annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

Vaultedge does not maintain a corporate network, intranet, or VPN, but instead opts to use SaaS and cloud applications hosted on the public internet and secured by TLS connections.

Boundaries of the System

The scope of this report includes the Services performed by Vaultedge. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

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

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

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 Vaultedge's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Vaultedge'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.

Vaultedge and its management team has 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

Vaultedge'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

Vaultedge'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

Vaultedge'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. Vaultedge's control environment reflects the philosophy of management. Vaultedge'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 Vaultedge 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

Vaultedge'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 updated as required.

Human Resources

Vaultedge'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

Vaultedge 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).

Vaultedge's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. Vaultedge identifies the underlying sources of risk, measures the impact to 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 Vaultedge Mortgage Automation software application, and management has implemented various measures designed to manage these risks.

- Vaultedge believes that effective risk management is based on the following principles:
- Senior management's commitment to the security of Vaultedge Mortgage Automation software application
- The involvement, cooperation, and insight of all Vaultedge 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 Vaultedge 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 Vaultedge Mortgage Automation software application. The Vaultedge 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 Vaultedge's Information Security Officer and the department or individuals responsible for the area being assessed. All Vaultedge 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

Vaultedge uses a number of vendors to meet its business objectives. Vaultedge 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.

Vaultedge 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, Vaultedge assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Vaultedge's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Vaultedge management meets with such vendors periodically to assess their performance, security concerns, and their services. 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, Vaultedge identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. Vaultedge'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.

Information and Communication

Vaultedge 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, Vaultedge 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 are maintained and made available to users on the company website.

Monitoring Controls

Vaultedge'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 is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Disclosure of Incidents

There were no system incidents as of August 11, 2022, 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.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Vaultedge's Vaultedge Mortgage Automation Software Application.

Subservice Organizations

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

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

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
Availability	A1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
		AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a register as appropriate, and reports results to leadership at least semi-annually.
		AWS has a process in place to review environmental and geo-political risks before launching a new region.

Subservice Organization – AWS		
Category	Criteria	Control
		Access to server locations is managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.

Subservice Organization – AWS		
Category	Criteria	Control
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.

Subservice Organization – Azure		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.

Subservice Organization – Azure		
Category	Criteria	Control
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.
		The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.
		Procedures for continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.
		A Datacenter Business Continuity Management (BCM) program to respond to Microsoft's Enterprise Business Continuance Initiative has been implemented and includes documented procedures for mapping processes to pre-defined enterprise functions, establishing recovery strategies as well as developing and conducting test scenarios that enable the BCM program to mitigate risks and vulnerabilities and respond to major disruptive events.

Subservice Organization – Azure		
Category	Criteria	Control
		A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.
		Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.
		Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined and backup data integrity checks are performed through standard restoration activities.
		Data corresponding to Azure is backed up to another region other than the primary data location and retained as per the retention policy.

Subservice Organization – Azure		
Category	Criteria	Control
		Production data on backup media is encrypted.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
		Customer data is retained and removed per the defined terms within the Microsoft Online Services Terms (OST), when a customer's subscription expires, or is terminated.
		Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

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

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Vaultedge's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Vaultedge's services to be solely achieved by Vaultedge's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Vaultedge's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Vaultedge.
2. User entities are responsible for notifying Vaultedge of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Vaultedge services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Vaultedge services.
6. User entities are responsible for providing Vaultedge with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Vaultedge of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Design of Controls and Results Thereof

Description of Design of Controls and Results Thereof

Relevant trust services criteria and Vaultedge related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Vaultedge controls were suitably designed to achieve the specified criteria for the Security, Availability, and Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, as of August 11, 2022.

Criteria Number	Description of Company Controls	Result
CC1.0 - Control Environment		
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.	Control is suitably designed
CC1.1.2	The company requires that new employees review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	Control is suitably designed
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	The company's Senior Management reviews and approves all company policies annually.	Control is suitably designed
CC1.2.2	The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Control is suitably designed
CC1.2.3	The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	Control is suitably designed
CC1.2.4	The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.5	The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Control is suitably designed
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	The company maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	Control is suitably designed
CC1.3.2	The company maintains job descriptions for client serving, IT and engineering positions to increase the operational effectiveness of employees within the organization.	Control is suitably designed
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The company ensures that new hires have been duly evaluated for competence in their expected job responsibilities.	Control is suitably designed
CC1.4.2	The company ensures that new hires go through a background check as part of their onboarding process.	Control is suitably designed
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The company has established a Security Awareness Training, and its contents are available for all staff on the company intranet.	Control is suitably designed
CC1.5.2	The company requires that new staff members complete Security Awareness Training upon hire, and that all staff members complete Security Awareness training annually.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.3	The company requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their Job responsibilities.	Control is suitably designed
CC1.5.4	The company requires that all staff members review and acknowledge company policies annually.	Control is suitably designed
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 company's systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Control is suitably designed
CC2.1.2	The company makes all policies and procedures available to all staff members via the company intranet.	Control is suitably designed
CC2.1.3	The company displays the most current information about its services on its website, which is accessible to its customers.	Control is suitably designed
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.	Control is suitably designed
CC2.2.2	The company requires that new staff members complete Security Awareness Training upon hire, and that all staff members complete Security Awareness training annually.	Control is suitably designed
CC2.2.3	The company requires that all staff members review and acknowledge company policies annually.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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.		
CC2.2.4	The company makes all policies and procedures available to all staff members via the company intranet.	Control is suitably designed
CC2.2.5	The company 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 company in the event there are problems.	Control is suitably designed
CC2.2.6	The company 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.	Control is suitably designed
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The company displays the most current information about its services on its website, which is accessible to its customers.	Control is suitably designed
CC2.3.2	The company has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the company in the event there are problems.	Control is suitably designed
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	The company has formally documented policies and procedures to govern risk management.	Control is suitably designed
CC3.1.2	The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The company 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	Control is suitably designed
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.	Control is suitably designed
CC3.2.3	The company 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.	Control is suitably designed
CC3.2.4	The company 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.	Control is suitably designed
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The company considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Control is suitably designed
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The company 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	Control is suitably designed
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.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.3	The company 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.	Control is suitably designed
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	The company'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.	Control is suitably designed
CC4.1.2	The company's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Control is suitably designed
CC4.1.3	The company's Senior Management reviews and approves all company policies annually.	Control is suitably designed
CC4.1.4	The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Control is suitably designed
CC4.1.5	The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	Control is suitably designed
CC4.1.6	The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	Control is suitably designed
CC4.1.7	The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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.		
CC4.1.8	The company reviews and evaluates all subservice organizations periodically, to ensure commitments to the company's customers can be met.	Control is suitably designed
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	The company 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 company in the event there are problems.	Control is suitably designed
CC4.2.2	The company's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Control is suitably designed
CC4.2.3	The company's Senior Management reviews and approves all company policies annually.	Control is suitably designed
CC4.2.4	The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Control is suitably designed
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	The company has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Control is suitably designed
CC5.1.2	The company's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Control is suitably designed
CC5.2.2	The company's Senior Management reviews and approves all company policies annually.	Control is suitably designed
CC5.2.3	The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	Control is suitably designed
CC5.2.4	The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	Control is suitably designed
CC5.2.5	The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	Control is suitably designed
CC5.2.6	The company's Senior Management reviews and approves the list of people with access to production console annually.	Control is suitably designed
CC5.2.7	The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Control is suitably designed
CC5.2.8	The company reviews and evaluates all subservice organizations periodically, to ensure commitments to the company's customers can be met.	Control is suitably designed
CC5.2.9	The company has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Control is suitably designed
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	The company makes all policies and procedures available to all staff members via the company intranet.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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.		
CC5.3.2	The company requires that all staff members review and acknowledge company policies annually.	Control is suitably designed
CC5.3.3	The company 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.	Control is suitably designed
CC5.3.4	The company has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Control is suitably designed
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	The company 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.	Control is suitably designed
CC6.1.2	The company maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Control is suitably designed
CC6.1.3	The company's Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to the company's system.	Control is suitably designed
CC6.1.4	The company's Senior Management or the Information Security Officer periodically reviews and approves the list of people with Administrative access to the company's system.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company 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.	Control is suitably designed
CC6.2.2	The company maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Control is suitably designed
CC6.2.3	Staff access to the company's systems are made inaccessible in a timely manner as a part of the offboarding process.	Control is suitably designed
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	The company maintains a matrix that outlines which system components should be accessible to staff members based on their role.	Control is suitably designed
CC6.3.2	Staff access to the company's systems are made inaccessible in a timely manner as a part of the offboarding process.	Control is suitably designed
CC6.3.3	The company 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.	Control is suitably designed
CC6.3.4	The company ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Control is suitably designed
CC6.3.5	Secure shell access to production systems is restricted to staff with access to production console.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The company 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.	The Criterion is carved out and the responsibility of the subservice organizations.
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	The company provides guidance on decommissioning of information assets that contain classified information in the Media Disposal Policy.	Control is suitably designed
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	The company requires that all staff members with access to Production console use Multifactor-authentication to access the console.	Control is suitably designed
CC6.6.2	The company requires that all staff members with access to the Change Management System use Multifactor-authentication to access the system.	Control is suitably designed
CC6.6.3	The company requires that all staff members with access to the Identity/Email Service use Multifactor-authentication to access the service.	Control is suitably designed
CC6.6.4	The company requires that all endpoints with access to production systems are protected by malware-protection software.	Control is suitably designed
CC6.6.5	The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Control is suitably designed
CC6.6.6	The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.7	The company requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity.	Control is suitably designed
CC6.6.8	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the company's cloud provider.	Control is suitably designed
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	The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Control is suitably designed
CC6.7.2	All production databases that store customer data are encrypted at rest.	Control is suitably designed
CC6.7.3	User access to the company's application is secured using https (TLS algorithm) and industry standard encryption.	Control is suitably designed
CC6.7.4	The company maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.	Control is suitably designed
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	The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Control is suitably designed
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 company's cloud provider.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Control is suitably designed
CC7.1.2	The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Control is suitably designed
CC7.1.3	The company'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.	Control is suitably designed
CC7.1.4	The company's production assets are continuously monitored to generate alerts and take immediate action where necessary.	Control is suitably designed
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	The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Control is suitably designed
CC7.2.2	The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Control is suitably designed
CC7.2.3	The company'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.	Control is suitably designed
CC7.2.4	The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Control is suitably designed
CC7.3.2	The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	Control is suitably designed
CC7.3.3	The company maintains a record of information security incidents.	Control is suitably designed
CC7.3.4	The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Control is suitably designed
CC7.3.5	The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	Control is suitably designed
CC7.3.6	The company'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.	Control is suitably designed
CC7.3.7	The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Control is suitably designed
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	The company's Information Security Officer performs an annual internal audit to assess and monitor the health of internal controls and shares the findings in an "Internal Audit Assessment" report with the Senior Management.	Control is suitably designed
CC7.4.2	The company has established an Incident Management and 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.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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.		
CC7.4.3	The company maintains a record of information security incidents.	Control is suitably designed
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Control is suitably designed
CC7.5.2	The company has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	Control is suitably designed
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	The company has a documented Change Management Policy, which is available to all Staff Members via the company intranet.	Control is suitably designed
CC8.1.2	The company uses a change management system to track, review and log all changes to the application code.	Control is suitably designed
CC8.1.3	The company maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.	Control is suitably designed
CC8.1.4	The company'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.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company 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 the company's service commitments and system requirements.	Control is suitably designed
CC9.1.2	The company 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	Control is suitably designed
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.	Control is suitably designed
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	The company 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 the company's service commitments and system requirements.	Control is suitably designed
CC9.2.2	The company has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.	Control is suitably designed
CC9.2.3	The company 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.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
A1.0 - Additional Criteria for Availability		
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	Control is suitably designed
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	The company has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	Control is suitably designed
A1.2.2	The company backs-up their production databases every hour.	Control is suitably designed
A1.2.3	The company's data backups are restored and tested annually.	Control is suitably designed
A1.2.4	The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Control is suitably designed
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Control is suitably designed
A1.3.2	The company's data backups are restored and tested annually.	Control is suitably designed
A1.3.3	The entity has documented a disaster recovery plan that is tested annually to ensure that recovery procedures are complete and accurate.	Control is suitably designed

Criteria Number	Description of Company Controls	Result
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	The company has a documented Confidentiality Policy, and makes it available for all staff on the company intranet.	Control is suitably designed
C1.1.2	The company requires that all new staff acknowledge the company's confidentiality policy as part of their onboarding.	Control is suitably designed
C1.1.3	The company has a documented Data Classification Policy, and makes it available for all staff on the company intranet.	Control is suitably designed
C1.1.4	All production databases that store customer data are encrypted at rest.	Control is suitably designed
C1.1.5	The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	Control is suitably designed
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	The company has a documented Data Retention Policy, and makes it available for all staff on the company intranet.	Control is suitably designed
C1.2.2	The company provides guidance on decommissioning of information assets that contain classified information in the Media Disposal Policy.	Control is suitably designed