SHAMAN

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

Shaman Platform

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

For the Period
April 1, 2022 to September 30, 2022

Together with
Independent Service Auditors' Report

SHAMAN

Table of Contents

I. Independent Service Auditors’ Report

SENSIBA SAN FILIPPO LLP
CERTIFIED PUBLIC ACCOUNTANTS AND BUSINESS ADVISORS

Independent Service Auditors' Report

To the Management of Shaman BV (Shaman)

Scope

We have examined Shaman's accompanying description of its Shaman Platform titled "Description of Shaman's Shaman Platform" throughout the period April 1, 2022 to September 30, 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*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that Shaman's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, 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*).

Shaman uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Shaman, to achieve Shaman's service commitments and system requirements based on the applicable trust services criteria. The description presents Shaman's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Shaman's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Shaman, to achieve Shaman's service commitments and system requirements based on the applicable trust services criteria. The description presents Shaman's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Shaman's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

Shaman 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 Shaman’s service commitments and system requirements were achieved. Shaman has provided the accompanying assertion titled “Assertion of Shaman Management” (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Shaman 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 and operating effectiveness 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 and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization’s system and the suitability of the design and operating effectiveness 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 or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

a. the description presents Shaman's Shaman Platform that was designed and implemented throughout the period April 1, 2022 to September 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that Shaman's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Shaman's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that Shaman's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Shaman's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Shaman, user entities of Shaman's Shaman Platform during some or all of the period April 1, 2022 to September 30, 2022, business partners of Shaman subject to risks arising from interactions with the Shaman Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Sensiba San Filippo LLP

San Jose, California

November 17, 2022

II. Assertion of Shaman Management

Assertion of Shaman Management

We have prepared the accompanying description of Shaman BV's (Shaman) Shaman Platform titled "Description of Shaman's Shaman Platform" throughout the period April 1, 2022 to September 30, 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)*. The description is intended to provide report users with information about the Shaman Platform that may be useful when assessing the risks arising from interactions with Shaman's system, particularly information about system controls that Shaman has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality (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).

Shaman uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Shaman, to achieve Shaman's service commitments and system requirements based on the applicable trust services criteria. The description presents Shaman's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Shaman's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Shaman's Shaman Platform that was designed and implemented throughout the period April 1, 2022 to September 30, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that Shaman's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Shaman's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period April 1, 2022 to September 30, 2022, to provide reasonable assurance that Shaman's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Shaman's controls operated effectively throughout that period.

Signed by Shaman Management

November 17, 2022

III. Description of Shaman’s Shaman Platform

SHAMAN

Description of Shaman's Shaman Platform

Company Background

Shaman was founded early 2015 with the objective to empower pharma content teams. Shaman is the leading sales content platform for Veeva with eDetailing, Email, Omnichannel and Sales Execution capabilities. This no-code, do-it-yourself experience helps Life Science companies to get the right content in front of their customers, increase Veeva adoption, and boost marketing omnichannel performance. The Shaman platform offers non Veeva customers with eDetailing solutions; this content can be distributed in a controlled way and presented on different devices. Shaman is a Veeva Technology Partner, and serves over 350 pharma content teams worldwide. The organization is based in Haarlem, The Netherlands with employees in over 10 countries worldwide.

Services Provided

Shaman offers a software-as-a-service (SaaS), Do It Yourself web application to create and distribute content in a controlled way. The platform comes with different packages and follows a team based or user based licensing model.

It empowers pharma content teams (both commercial and medical) as it makes the process to create content much easier and faster. The platform allows users to:

- Create interactive detail aids within 1-2 hours
- Create interactive detail aids within 1-2 hours for Veeva
- Create naming taxonomy for detail aids
- Create responsive email for Veeva, including Email templates, Email Fragments and Fragment Templates
- Create responsive email using design templates and predesigned blocks
- Create MLR documents from Email
- Bidirectional sync between Shaman and Veeva Vault Promomats for different scenario's like creation, updating documents, adding other documents
- Offer a statistical heatmap of detail aids
- Offer user management

Next to the software, Shaman offers an onboarding program including a dedicated Customer Success Manager for adoption and training, and an in-app chat for Support questions.

Principal Service Commitments and System Requirements

Shaman designs its processes and procedures related to its platform to meet its objectives for empowering pharma content teams. Those objectives are based on the service commitments that Shaman makes to user entities, the laws and regulations that govern the provision of analytics, and the financial, operational, and compliance requirements that Shaman has established for the services.

The analytics services of analytics are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Shaman operates.

Security 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 are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Shaman platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Components of the System

Infrastructure

Primary infrastructure used to provide Shaman's Services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Various Services, including EC2, IAM, Lambda, KMS, Load Balancer	Shaman Web application for logic, code, API and functions
AWS	S3, Glacier	Storage of Customer Content
AWS	RDS	Database of Application data incl Customer data
Google Workspace	Email, Cloud Storage	Employee email, calendar and storage of internal projects
Intercom	Customer support	Handling of customer tickets and inbox/ reply

Software

Primary software used to provide Shaman's Services system includes the following:

Primary Software		
Software	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
BitBucket	BitBucket	Application used to version control codebase and run CI/CD for deployments and testing
Wazuh	Wazuh	Security monitoring solution for threat detection, integrity monitoring, incident response and compliance

People

Shaman has a staff of around 50 employees organized in the following functional areas:

- Management Team. Executives to head up their own departments. Responsible for Strategy, HR, Legal and Finance
- Product and Development. These teams are responsible for product management, product development, DevOps and Infrastructure.
- Customer success. These teams are responsible for user adoption and usage of the platform in two teams: Customer Success Managers and Customer Support
- Business development. This team has access to the CRM systems and deals with new customers, expanding existing customers and renewals, including contracting and legal contracts.

Data

Data, as defined by Shaman, constitutes the following:

- Personal data (PII) of users and employees
- Contracts, quotes, invoices and financial reports
- Customer Content files
- System files
- Error logs

In general, data access is limited to only people that need access to this information.

Access to personal data of employees is very limited to a few employees on need to know basis.

Personal data of users is available only on production and limited accessible by few employees on need to know basis.

Processes, Policies and Procedures

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

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow Shaman employees physical access.

Logical Access

Shaman uses AWS for all hosting needs. Shaman leverages AWS's IAM for role-based security utilizing IAM groups.

For other cloud resources, employees sign on to using Google GSuite for Single Sign-On (SSO). Employees and other approved vendor personnel (who are not on Google GSuite) are also required to separately sign on to any systems or applications that do not implement Google SSO using passwords that conform to Shaman security policies.

Employees accessing cloud resources are required to enable token-based (OTP) multi-factor authentication as supported by each service provider. All cloud-based services are accessed through SSL-secured connections.

Prior to a new employee's start date, their manager creates a list of employee access to be granted. Access rules have been pre-defined based on the defined roles.
On a periodic basis, access rules for each role are reviewed by Shaman's Product and development team. As part of this process, the team lead/manager reviews access by privileged roles and requests modifications based on this review.

Computer Operations – Backups

Customer data is backed up by Shaman's engineering team. In the event of an exception, engineering 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

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Shaman monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Shaman evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- CPU utilization

Change Control

Shaman maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system (Jira) is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system

Version control software (Bitbucket) is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Shaman has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Shaman system owners review proposed operating system patches to determine whether the patches are applied. Customers and Shaman systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses.

Shaman utilizes security groups as stateful firewalls.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Shaman.

The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network.

Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed periodically by AWS Inspector in accordance with the Shaman Vulnerability and Patch Management Policy.

Amazon Inspector is an AWS-developed vulnerability management service that has built-in support for applicable AWS resources. Amazon Inspector Provides a contextual Inspector score and Common Vulnerability Scoring System (CVSS) v2 and v3 scores from both National Vulnerability Database (NVD) and vendors. All scans are automatically performed based on events. All workloads are initially scanned upon discovery and subsequently rescanned.

Boundaries of the System

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 Shaman’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Shaman’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, as well as by example.

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

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

Commitment to Competence

Shaman's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

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

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

Management's Philosophy and Operating Style

Shaman's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

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

Organizational Structure and Assignment of Authority and Responsibility

Shaman's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes 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.

Shaman's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It 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.

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

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

Human Resource Policies and Practices

Shaman'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 its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Shaman's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- Employees are expected to take security awareness trainings annually and upon hire.

Risk Assessment Process

Shaman's risk assessment process identifies and manages risks that could potentially affect Shaman's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility.

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

- Sensitive data
- Codebase
- People
- Production services
- Physical security

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Shaman's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Shaman addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Shaman's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Shaman's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Shaman, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Shaman personnel via slack messages.

Specific information systems used to support Shaman's system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Shaman's management performs monitoring activities 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. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

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

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

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 Shaman's Shaman Platform.

Subservice Organizations

Shaman BV'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 Shaman's services to be solely achieved by Shaman's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Shaman.

The following subservice organization controls should be implemented by AWS 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.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are 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.
Availability	A1.2	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.

Subservice Organization – AWS		
Category	Criteria	Control
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		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, and redundant power supplies.
		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.

Shaman 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, Shaman 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

Shaman'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 Shaman's services to be solely achieved by Shaman's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Shaman'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 Shaman.
2. User entities are responsible for notifying Shaman 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 Shaman 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 Shaman services.
6. User entities are responsible for providing Shaman with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Shaman of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. Description of Criteria, Controls, Tests and Results of Tests

Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Shaman 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 Shaman's controls were suitably designed and operating effectively to achieve the specified criteria for the Security, Availability, Confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period April 1, 2022 to September 30, 2022.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Shaman activities and operations and inspection of Shaman documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Shaman controls, this test was not listed individually for every control in the tables below.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
The company has established a Code of Conduct and requires all employees to agree to it. Management monitors employees' acceptance of the code.	CC1.1.1	Inspected the policy that documents the company's Code of Conduct to determine that it was in place and provides guidance on workforce conduct standards.	No exceptions noted
		Inspected the signed Code of Conduct for a sample of employees to determine that they had agreed to the company's Code of Conduct.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of 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.			
The company demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	CC1.2.1	Inspected the Code of Conduct, Information Security Policy, and evidence of management's review of the policies, to determine that the company demonstrates a commitment to integrity and ethical values.	No exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
Company management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and escalation. The organizational charts are made available to employees through the company's HR Information System to facilitate communication in their role with the company.	CC1.3.1	Inspected the company's HR Information System to determine that organizational charts are accessible for employees.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
All positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	CC1.4.1	Inspected a sample engineer job description from the company to determine that all positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the company.	No exceptions noted
Reference checks are performed on new hires. The results are reviewed by HR and appropriate action is taken if deemed necessary.	CC1.4.2	Inspected a sample new hire contract to determine that new hires are required to sign a contract upon hire.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The company has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete these trainings annually.	CC1.5.1	Inspected the security awareness training completion for a sample of employees to determine that the company has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the company's security policies and procedures.	No exceptions noted
Management has approved the company's security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC1.5.2	Inspected the signed security policies for a sample of employees to determine that all employees had agreed to the security policies.	No exceptions noted
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	CC2.1.1	Inspected the Vanta tool configurations to determine that the company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company control environment and alerts management when internal control and security issues arise.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of 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.			
The company has policies and procedures in place to establish access control of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must agree to the Access Control Policy on hire.	CC2.2.1	Inspected company records to determine that a policy that establishes the access control of information assets is in place, has been approved by management, and is accessible to employees.	No exceptions noted
		Inspected the signed Access Control policy for a sample of employees to determine that they had agreed to the company's Access Control Policy.	No exceptions noted
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
The company maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	CC2.3.1	Inspected the company Privacy Policy to determine that it is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	No exceptions noted
The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Where the Terms of Service may not apply, the company has Client Agreements or Master Service Agreements in place.	CC2.3.2	Inspected the company Public Acceptable Use Policy to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
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.			
The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	CC3.1.1	Inspected the Risk Management Policy to determine that the company has a formal program for identifying and managing risks.	No exceptions noted
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
The company maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	CC3.2.1	Inspected the security risk assessment, which includes the risks, prioritization, and action plans to determine that the company maintains a risk register that continuously documents risks facing the company.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
The company identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.).	CC3.3.1	Inspected the fraud assessment to determine that the entity identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.)	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	CC3.4.1	Inspected the Vanta tool configurations to determine that the company uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the company control environment and alerts management when internal control and security issues arise.	No exceptions noted
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
Monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity.	CC4.1.1	Inspected the monitoring dashboard to determine that monitoring software is used to identify and evaluate ongoing system performance, changing resource utilization needs, and unusual system activity.	No exceptions noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
The company has an established Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC4.2.1	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
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.			
The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	CC4.2.2	Inspected the contact form to determine that the company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
A list of the company's system components is maintained for management's use in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	CC5.1.1	Inspected the inventory listing of information assets the company maintains in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
The company has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in company infrastructure.	CC5.2.1	Inspected the vulnerability scan to determine that the company has implemented a vulnerability management program to detect and remediate system vulnerabilities.	No exceptions noted
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC5.2.2	Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of 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.			
Management has approved the company's security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC5.3.1	Inspected the company's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted
		Inspected records of the company's security policies to determine that all employees have agreed to them.	No exceptions noted
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.1	Inspected the configuration for the company's infrastructure provider to determine that permissions are assigned to groups.	No exceptions noted
		Inspected the configuration for the company's infrastructure tool to determine that employees have unique accounts on the service.	No exceptions noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
Access to infrastructure and code review tools is granted to new employees subsequent to the initial request.	CC6.2.1	Inspected the employee access tracker for a sample of employees to determine that employee access to infrastructure is granted.	No exceptions noted
Access to infrastructure and code review tools is removed as a component of the termination process.	CC6.2.2	Inspected the termination checklist for a sample of terminated employees to determine that employee access to infrastructure is removed as a component of the termination process.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
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.			
Access is restricted to authorized personnel. Access approval and modification to access list are logged. Access is removed when appropriate.	CC6.3.1	Inspected access lists for the infrastructure provider to determine that access is limited to authorized personnel and removed when appropriate.	No exceptions noted
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
The company relies on AWS's physical and environmental controls, as defined and tested within AWS SOC 2 efforts.	CC6.4.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization (AWS).
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.			
Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	CC6.5.1	Inspected the Data Management Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Access to sensitive systems and applications requires two factor authentication in the form of user ID, password, OTP and/or certificate.	CC6.6.1	Inspected all user accounts with access to company infrastructure to determine that each is configured with MFA.	No exceptions noted
The company implements firewalls and configures them to protect against threats from sources outside its system boundaries.	CC6.6.2	Inspected the firewall configuration to determine that access control lists were used to filter unwanted network traffic.	No exceptions noted
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
Company management ensures that all company-issued laptop hard drives are encrypted using full disk encryption.	CC6.7.1	Inspected employee computers to determine that each was protected with full-disk encryption.	No exceptions noted
Customer data stored in databases is encrypted at rest.	CC6.7.2	Inspected the database configurations to determine that data is encrypted at rest.	No exceptions noted
Encryption is used to protect user authentication and administrator sessions of the internal admin tool transmitted over the Internet.	CC6.7.3	Inspected the encryption configurations to determine that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The company deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	CC6.8.1	Inspected the antivirus configurations to determine that the company deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	No exceptions noted
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	CC7.1	Inspected the vulnerability management tool to determine that the company has established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.	No exceptions noted
		Inspected the penetration test report to determine that a penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	CC7.2.1	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
		Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
Remediation of security deficiencies are tracked through internal tools.	CC7.3.1	Inspected the Incident Response Plan to determine that security issues are tagged and prioritized accordingly.	No exceptions noted
Security deficiencies tracked through internal tools are closed once remediated.	CC7.3.2	Inspected the Incident Response Plan to determine that security issues are tracked through internal tools and closed once remediated.	N/A - Non-Occurrence (No security and privacy incidents during the period)
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.			
Remediation of security deficiencies are tracked through internal tools.	CC7.4.1	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of 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.			
Security deficiencies tracked through internal tools are closed once remediated.	CC7.4.2	Inspected the Incident Response Plan to determine that security issues are tagged and prioritized accordingly.	N/A - Non-Occurrence (No security and privacy incidents during the period)
The company has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	CC7.4.3	Inspected the Incident Response Plan to determine that security issues are tracked through internal tools and closed once remediated.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
The company has created a Disaster Recovery Plan to define the organization's procedures to recover information technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident.	CC7.5.1	Inspected the Company's Disaster Recovery Plan to determine that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
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.			
The company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	CC8.1.1	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
		Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted
System changes must be approved by an independent technical resource prior to deployment to production.	CC8.1.2	Inspected a sample change ticket to determine that system changes must be approved by an independent technical resource prior to deployment to production.	No exceptions noted
		Inspected a sample change ticket to determine that application changes are tested prior to deployment to production.	No exceptions noted
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The company's Risk Management Policy describes the processes the company has in place to identify new business and technical risks and how frequently those risks are mitigated.	CC9.1.1	Inspected the Risk Management Policy to determine that the company has a formal program for identifying and managing risks.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The company has created a Business Continuity Plan to define the criteria for continuing business operations for the organization in the event of a disruption.	CC9.1.2	Inspected the company's Business Continuity Plan to determine that it defined an operational and organizational strategy in the event of a disruption and has been updated in the past year.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company's team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	CC9.2.1	Inspected the written policy governing the use of external service providers to determine that the sub-service organization approval process includes collecting and reviewing the provider's SOC report(s).	No exceptions noted
The company has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	CC9.2.2	Inspected the company's vendor management tool to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	No exceptions noted
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.			
Processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	A1.1.1	Inspected the monitoring dashboard to determine that processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The company relies on AWS's physical and environmental controls, as defined and tested within AWS SOC 2 efforts.	A1.2.1	Not Applicable - Control is Carved Out	No exceptions noted
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	A1.3.1	Inspected the Backup policy and database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
Management has approved the company's security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	C1.1.1	Inspected the company's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted
		Inspected records of the company's security policies to determine that all employees have agreed to them.	No exceptions noted
Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	C1.1.2	Inspected the data classification and data deletion policies to determine that procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor’s Test of Controls	Result
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	C1.2.1	Inspected the data deletion policy to determine that procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	No exceptions noted