SOC 1 Report

For

Noosh Applications Services

A Type 2 Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

For the Period November 1, 2019, to October 31, 2020

Prepared in Accordance with the
AICPA SSAE No. 18 Standard

Attestation and Compliance Services

This report is intended solely for use by the management of Noosh, Inc., its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Noosh, Inc.:

Scope

We have examined Noosh, Inc.'s ("Noosh" or "service organization") description of its Noosh applications services system for managing and delivering marketing print procurement and project management software throughout the period November 1, 2019, to October 31, 2020 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of Noosh believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Noosh applications services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Noosh's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Noosh uses various subservice organizations for data center and cloud hosting services. The description includes only the control objectives and related controls of Noosh and excludes the control objectives and related controls of the subservice organizations. The description also indicates whether certain control objectives specified by Noosh can be achieved only if complementary subservice organization controls assumed in the design of Noosh's controls are suitably designed and operating effectively, along with the related controls at Noosh. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

In Section 2, Noosh has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Noosh is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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 the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2019, to October 31, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in misstatements in managing and delivering marketing print procurement and project management software. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

Opinion

In our opinion, in all material respects, based on the criteria described in Noosh's assertion in Section 2,

a. the description fairly presents the Noosh applications services system that was designed and implemented throughout the period November 1, 2019, to October 31, 2020;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2019, to October 31, 2020, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of Noosh's controls throughout the period November 1, 2019, to October 31, 2020; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2019, to October 31, 2020, if, as applicable, complementary subservice organization and user entity controls assumed in the design of Noosh's controls operated effectively throughout the period November 1, 2019, to October 31, 2020.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of Noosh, user entities of Noosh's applications services system during some or all of the period November 1, 2019, to October 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Schellman & Company, LLC

Tampa, Florida
October 29, 2020

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Noosh, Inc.'s ("Noosh") Noosh applications services system for managing and delivering marketing print procurement and project management software throughout the period November 1, 2019, to October 31, 2020 (the "description"), for user entities of the system during some or all of the period November 1, 2019, to October 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

Noosh uses various subservice organizations for data center and cloud hosting services. The description includes only the control objectives and related controls of Noosh and excludes the control objectives and related controls of the subservice organizations. The description also indicates whether certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Noosh's controls are suitably designed and operating effectively, along with related controls at Noosh. The description does not extend to controls of the user entities.

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

a. the description fairly presents the Noosh applications services system made available to user entities of the system during some or all of the period November 1, 2019, to October 31, 2020, for managing and delivering marketing print procurement and project management software as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

    i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, as applicable:

        (1) the types of services provided including, as appropriate, the classes of transactions processed;

        (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities of the system;

        (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

        (4) how the system captures and addresses significant events and conditions, other than transactions;

        (5) the process used to prepare reports or other information provided for entities;

        (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

        (7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the Noosh's controls; and

(8) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided;

ii. includes relevant details of changes to the Noosh applications services system during the period covered by the description; and

iii. does not omit or distort information relevant to the scope of the Noosh applications services system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Noosh applications services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period November 1, 2019, to October 31, 2020, to achieve those control objectives if, as applicable, subservice organizations and user entities applied complementary controls assumed in the design of Noosh's controls throughout the period November 1, 2019, to October 31, 2020. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of Noosh;

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3

Description of the System

OVERVIEW OF OPERATIONS

Company Background

Noosh, Inc. was founded in 1998 and is a California-based company with its headquarters in Mountain View, California. The Noosh application helps enterprises deliver marketing print procurement and project management software by streamlining business operations and enabling collaboration with vendors. Noosh's product and marketing services allow customers to manage digital and print assets, cost structures, budgets, procurements, projects, and team interaction using an integrated cloud-based approach.

Description of Services Provided

The Noosh application provides customers with functionality to collaborate with coworkers and suppliers on content marketing projects. Noosh customers have the ability to:

- Invite their coworkers and suppliers
- Admins have the ability to change roles and privileges
- Send/receive orders (no financial transactions occur in the software)
- Send/receive estimates/quotes
- Send/receive invoices/proposals
- Create schedules and tasks
- Create budgets
- Exchange and proof files
- Run reports to track datasets within the application
- Integrate with common enterprise resource planning (ERP) systems
- Deliver notifications to customers when actions are performed, and the subsequent actions are also logged into a project event list for added visibility

Requests for services are initiated and authorized by user entities through self-service functions on the Noosh application website. Customer requests are also recorded and tracked through self-service functions on the website. Customer complaints are recorded, organized, and tracked to resolution using the Zendesk customer relationship management (CRM) system.

The Noosh application customer web interface offers the following content marketing features for enterprise marketing teams:

- SmartForms – customize or create fully-collaborative, fully-reportable product, and service specifications to share with suppliers; SmartForms also generates data-rich reports.
- Real-time analytics – reports on the status of projects with real-time process analytics and real-time reporting to understand project processes as well as project outcomes.
- Business process reporting – includes reporting capabilities for time-based service level agreements (SLA), sourcing strategies, tasks, estimates, and an outsourcing profitability analysis.
- Supplier management – maintains a database of current suppliers and how they're performing. Rates supplier performance using the configurable criteria including cost, quality, on-time delivery, and customer service to develop quarterly reviews.
- File management – used to upload and share files up to five gigabytes (GB) per file and assign tags to keep them organized in multiple categories.
- Messaging – offers project-level messaging to stay in sync about changing project requirements.

Noosh's application services environment is an information technology general control (ITGC) system, and user entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within Noosh's application services; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Boundaries of the System

The scope of the review is limited to the Noosh applications system performed at the Mountain View, California, facility. The specific control objectives and related control activities included within the scope of this engagement can be found in Section 4 of this document.

Subservice Organizations

Noosh utilizes the data center hosting services provided by Wave and the cloud hosting services provided by Amazon Web Services, Inc. (AWS). Noosh's application services system is 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 control objectives related to Noosh's application services system to be solely achieved by Noosh's control activities. Accordingly, subservice organizations, in conjunction with the application services system, should establish their own internal controls or procedures to complement those of Noosh.

Complementary Controls at Subservice Organizations

The following complementary subservice organization controls should be implemented by subservice organizations to provide additional assurance that the specified control objectives described within this report are achieved:

Control Activities Expected to be Implemented at Subservice Organizations	Related Control Objective
AWS is responsible for providing the underlying network infrastructure which allows Noosh to maintain redundancy.	Computer Operations
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where Noosh's systems reside.	Computer Operations Information Security Data Communications
AWS is responsible for providing the underlying network infrastructure for providing secure connectivity.	Data Communications

Significant Changes During the Review Period

No significant changes to the application services system occurred during the review period.

Functional Areas of Operations

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Information technology (IT) operations – manages, monitors, and supports information and systems for operational effectiveness, integrity, availability, problem management, change management, and compliance while protecting systems from unauthorized access and misuse.
- Development team – responsible for developing and testing application changes and providing technical support services to the IT operations team for the Noosh applications system.

Infrastructure

Noosh applications systems are designed for cloud operations and service delivery. The system platform is comprised of a three-tier architecture including the web application, production application servers, and database

servers. The web application tier uses custom-developed application software. Noosh production application servers are hosted on AWS Elastic Compute Cloud (EC2) with secure Virtual Private Cloud (VPC), virtual machines, and AWS Relational Database Service (RDS). Oracle 11g is used by the database server supporting the Noosh application and database access is managed through the Oracle database appliance (ODA). The Noosh office facility network domain is supported by Microsoft Windows Active Directory.

Noosh utilizes the following applications to support the services provided:

- Pingdom server uptime and performance monitoring
- An internally developed application called Noosh Knowledge Based (NKB) to track change control activities
- Zendesk CRM to receive, organize, and track customer complaints/comments through to resolution
- Jira tickets to track any issues needing to be addressed by engineering through to resolution
- Truesight monitoring tool by BMC Software
- AWS CloudWatch for monitoring production servers
- PagerDuty for incident notification and 24x7 support escalation
- ThousandEyes for monitoring the service network across the globe
- New Relic for application performance management

Data Management

Noosh utilizes data from Pingdom to generate SLA uptime reports for customer review. Noosh also offers self-service reporting tools on the Noosh application website for customers to have the ability to report on and analyze any dataset within the application, either by using our pre-built reports or by creating custom reports. Additionally, Noosh provides an activity log within the application to track actions taken within a project.

CONTROL ENVIRONMENT

The control environment at Noosh is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

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 Noosh's control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Noosh's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. These 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.

- Organizational policy statements and codes of conduct are documented and communicated to employees.
- The employee policy and procedures manual contain organizational policy statements and codes of conduct to which employees are required to adhere.
- Policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.

- Employees must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.

Board of Directors and Audit Committee Oversight

Noosh's control consciousness is influenced significantly by its board of directors and audit committee participation. The board of directors and audit committee oversee management activities and meet on a quarterly basis to discuss operational issues. At this meeting, management presents the status of the current operation and the strategic plan going forward. The board asks for questions and clarification on any outstanding topics and gives management feedback, which is taken into account when running the company.

Organizational Structure and Assignment of Authority and Responsibility

Noosh's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Noosh's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility in addition to structured lines of reporting. Noosh has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Noosh'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 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 that 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, responsibility, and lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Commitment to Competence

Noosh management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Noosh's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that the service organization has implemented in this area are described below.

- Skills tests are administered to Noosh employee candidates to ensure only competent candidates are hired.
- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.

Accountability

Noosh'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. Management is periodically briefed on regulatory and industry changes affecting services provided.

Noosh human resources (HR) policies and practices relating 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.

- Pre-hire screening procedures are in place to govern the new hire process.
- Management performs evaluations for each employee on a quarterly basis.
- Employee termination procedures are in place to govern the termination process.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the service organization's system. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

Risk Identification

In order to identify the risk associated with each control objective, a risk level assessment is performed on the control activities found within the respective control objectives. For example, a control objective such as Computer Operations is comprised of individual control activities. Each control activity is reviewed by management and departmental personnel to determine whether Noosh's ability to adhere to the control activity as stated exists and the probability that Noosh will maintain adherence using a grading system of high, medium, and low.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, fraud incentives, pressures, opportunities, and attitudes for employees
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Noosh's methodology for analyzing risks varies, largely because many risks are difficult to quantify. The process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

Management identifies risk and remediation plans at weekly management meetings. Risks are also assessed and evaluated at these meetings, which includes management and risk operations personnel. As risks are assessed and analyzed, policies, and procedures to mitigate risks are established and implemented.

Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which Noosh strives to achieve its business objectives. Noosh has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Noosh evaluate the relationships between business processes and the use technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Noosh personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed and improved when necessary.

Noosh's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Computer Operations

Control Objective: Control activities provide reasonable assurance that application and data files for the Noosh applications are backed up in a timely manner and securely stored.

Noosh applications store customer data within an Oracle database hosted in a Wave data center in Santa Clara or within AWS RDS databases in the us-west-1 or eu-central-1 regions. Noosh utilizes automated backup scripts to perform backups of the Oracle database on a continuous basis. The Oracle database is first backed up locally and then is replicated to an AWS us-east (N. Virginia) data center. Noosh has contracted a third-party support company, Database Specialists Inc., to monitor the status of the backup jobs and notify Noosh IT operations personnel in the event of a failure. Noosh uses RDS Multi-AZ DB Instances. Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Noosh personnel monitor the status of backups on a daily basis. The ability to access the backup data stored in the AWS data center is restricted to the vice president of engineering (VPE) and an engineer. IT operation personnel perform backup restoration tests on for the Oracle database hosted in the Wave data center on at least an annual basis to help ensure the validity of backup data. Noosh has configured the AWS RDS database to run multi-availability zone mode to help ensure AWS RDS databases will failover automatically.

Control Objective: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

IT operations personnel utilize various enterprise monitoring applications to monitor the health and availability of the production environment. AWS provides built-in monitoring tools to monitor the various production application servers hosted in that environment. Zabbix is utilized to monitor the production servers and database server and Pingdom is used to monitor uptime for the Noosh Enterprise application portal. Monitoring systems provide real-time alerts that are sent to IT operations personnel via e-mail.

Service agreements are in place with Oracle to provide additional support and maintenance for the ODA residing in the Wave Business data center. These agreements are renewed on an annual basis. Noosh has also contracted Database Specialists to perform health and availability monitoring for the production database.

Information Security

Control Objective: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

Noosh management has implemented policies and procedures to guide personnel in performing information security activities. Employees are required to sign a security acknowledgment of policies including, but not limited to, acceptable use, encryption, passwords, employee exit, and server security. Requests for system access require approval from a manager prior to granting access to the Noosh network domain and network access privileges are reviewed annually.

When employees are terminated, HR personnel and/or the departmental manager notify IT personnel of the termination via e-mail. Systems administration personnel then revoke system user accounts assigned to terminated employees.

Authentication and access controls have been implemented at each layer of the Noosh environment including the network domain, production application server operating systems, production databases, and web application. Specifically, users are required to authenticate via an authorized active directory user account and password when accessing the network domain and administrative network domain access is further restricted to user accounts within the Domain Admins user access group. Users are required to authenticate via an authorized operating system user account and password when accessing production application or database servers and administrative production application or database server access is further restricted to user accounts within each server's operating system administrative user access groups. Access to Oracle and RDS databases is authenticated through a user account and a strong password. AWS management console users, including administrative users, are required to authenticate via an authorized AWS user account and password when accessing the AWS management console Password minimum length requirements have been implemented and are systematically enforced at the network domain, production application server, production database, AWS management console, and Noosh application levels. Additional password controls including expiration intervals, complexity requirements, minimum history, and account lockout threshold have also been implemented and are systematically enforced at the network domain and Noosh application levels.

Internal Noosh application users, including administrative users, are required to authenticate via an authorized Noosh application user account and password when accessing the Noosh application.

Data Communications

Control Objective: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

A software-based firewall system is in place and utilized to protect the production environment and data. The firewall resides on the network perimeter and analyzes data and packets routed to the production environment. External Internet traffic is required to pass through the firewall to communicate with the production servers. Any type of connection that is not explicitly authorized by the firewall will be denied. Network address translation (NAT) rules are in place to translate internal Internet Protocol (IP) addresses to publicly routable IP addresses. Administrator access within the firewall system is restricted to IT operations personnel and a third-party contractor.

AWS security groups are in place to provide additional perimeter security for the production application server environment. The security groups monitor incoming network traffic by analyzing the data packets and determining whether they should be allowed through based on the ruleset. The ability to create, modify, and delete the security groups is restricted to authorized IT operations personnel. IT operations personnel are required to authenticate to the AWS management console via a user account and password in order to perform any modifications to the security groups.

Remote access to the production environment is restricted via an encrypted virtual private network (VPN) connection. Communication to the AWS production environment is encrypted via advanced encryption standard (AES) 256-SHA1 and connections to the Wave Business data center production environment are encrypted via AES128-cipher block chaining (CBC) algorithms. Before a user can establish a VPN connection, they must authenticate via their network domain user account and password. Users establishing a VPN connection to the AWS or Wave Business data center production environments must also possess a security certificate.

To protect data while in transit, Noosh's hosted website for the Noosh Enterprise application transmits data utilizing Hypertext Transfer Protocol Secure (HTTPS) with transport layer security (TLS) encryption.

Application Change Control

Control Objective: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

Noosh has established documented procedures to guide personnel in performing application change activities. Sprint planning meetings are held prior to the commencement of each sprint to plan and prioritize upcoming development projects. During these meetings, stakeholders will evaluate the feasibility of proposed changes and determine which enhancements or features should be prioritized in the upcoming release. To assist with the management of changes, a change management tracking system is utilized to centrally maintain, manage, and monitor change control activities.

An Agile development methodology is used for application development activities where enhancements and new feature development projects are compiled into sprints. Minor enhancements and patches are released bi-weekly and larger development projects including new features are released monthly. The release implementation team meets on a weekly basis to prioritize and approve tasks to be included in the upcoming release. Version control software is utilized to restrict access to source code and provide rollback capabilities. Once the software development standards have been met, the code is peer-reviewed prior to being merged into the main branch. The version control software is configured to prevent code from being merged into the master branch without first being peer-reviewed. The ability to modify code within the version control software is restricted to development personnel.

Quality assurance (QA) personnel perform functional testing for application changes prior to submitting the change for review and approval. Changes are developed and tested in environments that are logically separate from production. Application changes are reviewed and approved prior to being implemented. Further, a version monitoring script to is utilized to monitor for changes to the production environment and sends daily e-mail notifications to members of the IT department. The notifications are reviewed upon receipt and the required action is taken if deemed necessary.

Information and Communication Systems

Relevant Information

Information is necessary for Noosh to carry out internal control responsibilities to support the achievement of its objectives related to the Noosh application. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The Noosh application allows enterprises to deliver on marketing procurement by streamlining operations and enabling collaboration with vendors. The company's products and marketing services partners manage digital and

print assets, cost structures, budgets, procurements, projects, and team interaction using an integrated cloud-based approach.

Communication

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within Noosh. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts and employee handbooks are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

MONITORING

Monitoring Activities

Noosh's management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, customer conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. The greater the degree and effectiveness of ongoing monitoring, the less the need is for separate evaluations. Management determines the need for separate evaluations by consideration given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring.

Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary to help ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of Noosh's ongoing monitoring activities include the following:

- Management reviews the annual service auditor's report for the cloud hosting services provided by AWS and the data center hosting services provided by Wave on an annual basis.
- In carrying out its regular management activities, operations management obtains evidence, such as e-mail alerts, to ensure that the system of internal control continues to function.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Training, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- Personnel is briefed on organizational policy statements and codes of conduct to communicate entity values.
- Support personnel utilizes a ticketing system to manage systems infrastructure issues. Tickets are assigned to support personnel based on the incident severity, priority, and urgency.
- Management utilizes enterprise monitoring applications to monitor the performance and availability of production servers and network devices.

- The enterprise monitoring applications are configured to send automated e-mail alert notifications to support personnel when pre-defined thresholds are exceeded on monitored production servers and network devices.

Separate Evaluations

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Monitoring of Subservice Organizations

Management's description of the service organization's system and the scope of the service auditor's engagement should include a description of service organization's controls that monitor the effectiveness of controls at the subservice organization. These may include some combination of (1) ongoing monitoring to determine that potential issues are identified timely and (2) separate evaluations to determine that the effectiveness of internal control is maintained over time. Such monitoring activities may include

- Reviewing System and Organization Control (SOC) Type 1 or Type 2 examination reports on the subservice organization's system; and
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Reporting Deficiencies

Deficiencies in management's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Complementary Controls at User Entities

Noosh's application services system is 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 of the control objectives related to Noosh's application services system to be solely achieved by Noosh's control activities. Accordingly, user entities, in conjunction with the application services system, should establish their own internal controls or procedures to complement those of Noosh.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls for configuring Noosh application password parameters and complexity requirements settings.	Information Security
User entities are expected to implement controls for user administration and authorization activities for the Noosh application.	

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls for immediately notifying Noosh of any actual or suspected information security breaches, including compromised user accounts.	
User entities are expected to implement controls for ensuring the security and integrity of any data or information transmitted via their service or over the Internet.	Data Communications
User entities are expected to implement controls for determining whether Noosh's security infrastructure is appropriate for their needs and notifying Noosh of any requested modifications.	
User entities are expected to implement controls for notifying Noosh of requested modifications to application functionality or features.	Application Change Control

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Noosh application services system provided by Noosh. The scope of the testing was restricted to the Noosh application services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period November 1, 2019, through October 31, 2020.

Tests of Operating Effectiveness

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

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

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

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

Sampling

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

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the "Complementary Controls at User Entities" within Section 3. Control considerations that should be implemented by subservice organizations in order to complement the control activities and achieve the stated control objective are presented in the "Complementary Controls at Subservice Organizations" within Section 3.

COMPUTER OPERATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that application and data files for the Noosh applications are backed up in a timely manner and securely stored.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	Programmed backup scripts are in place to perform scheduled backups of production data and systems on a daily basis.	Inspected the backup configurations for a sample of production databases and example backup logs generated during the review period to determine that programmed backup scripts were in place to perform scheduled backups of production data and systems on a daily basis for each database sampled.	No exceptions noted.
1.02	Production data is replicated to a backup server in an off-site facility or a separate availability zone on a daily basis.	Inspected the data replication configurations for a sample of production databases and example replication logs generated during the review period to determine that production data was replicated to a backup server in an off-site facility on a daily basis for each database sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.03	The chief financial officer (CFO) and IT personnel review status reports on a daily basis as evidence that a third-party provider monitors the status of the production databases and programmed backup scripts.	Inspected the third-party support provider contract, the most recent annual invoice and backup status summaries for a sample of dates during the review period to determine that a third-party provider monitored the status of the production databases and programmed backup scripts and distributed a daily summary of backup statuses for each date sampled.	No exceptions noted.
1.04	The ability to access backup data is restricted to user accounts accessible by persons holding the following positions: • Vice president (VP) of engineering • Engineer	Inquired of the engineer regarding backup data access to determine that the ability to access backup data was restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer	No exceptions noted.
		Inspected the backup data user account listing to determine that the ability to access backup data was restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer	No exceptions noted.
1.05	IT operations personnel perform data restorations on an annual basis to help ensure that data can be restored from backups.	Inquired of the engineer regarding data restorations to determine that IT operations personnel performed data restorations on an annual basis to help ensure that data can be restored from backups.	No exceptions noted.
		Inspected the results from the most recent data restoration to determine that IT operations personnel performed a data restoration during the review period.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	Enterprise monitoring applications are utilized to monitor the performance and availability of production servers and network devices.	Inspected the enterprise monitoring application configurations to determine that enterprise monitoring applications were utilized to monitor the performance and availability of production servers and network devices.	No exceptions noted.
2.02	The enterprise monitoring applications are configured to send e-mail notifications to IT personnel when pre-defined thresholds are exceeded on monitored production servers and network devices.	Inspected the enterprise monitoring application configurations and example e-mail notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail notifications to IT operations personnel when pre-defined thresholds were exceeded on monitored on production servers and network devices.	No exceptions noted.
2.03	IT personnel maintain service agreements for certain production hardware and software systems.	Inspected the third-party service agreement, the most recent annual service agreement invoice, and an example of the most recent e-mail alert from the database specialist to determine that IT personnel maintained service agreements for certain production hardware and software systems.	No exceptions noted.
2.04	The CFO and IT personnel review status reports on a daily basis as evidence that a third-party provider monitors the status of the production databases and programmed backup scripts.	Inspected the third-party support provider contract, the most recent annual invoice and backup status summaries for a sample of dates during the review period to determine that a third-party provider monitored the status of the production databases and programmed backup scripts and distributed a daily summary of backup statuses for each date sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.05	Linux-based technology and software architecture is in place which minimizes the risk of production servers being infected by computer viruses, malicious code, and unauthorized software.	Inspected the Linux configurations for a sample of production servers to determine that Linux-based technology and software architecture was in place which minimizes the risk of production servers being infected by computer viruses, malicious code, and unauthorized software for each server sampled.	No exceptions noted.
2.06	An internal tracking tool is utilized to log production incidents that include, but are not limited to, the following: • Incident description • Impact (down time) • Issue type • Root cause • Resolution	Inspected the data center incident log for a sample of incidents generated during the review period to determine that an internal tracking tool was utilized to log production incidents that included the following: • Incident description • Impact (down time) • Issue type • Root cause • Resolution	No exceptions noted.

INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.01	Documented policies and procedures are in place to guide personnel in performing information security activities including, but not limited to, the following: • Acceptable use • Encryption • Passwords • Employee exit • Server security	Inspected the information security policies to determine that policies and procedures were in place to guide personnel in performing information security activities that included the following: • Acceptable use • Encryption • Passwords • Employee exit • Server security	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.02	Employees are required to sign a security acknowledgment form indicating their understanding of company security policies upon hire and annually thereafter.	Inspected the signed security acknowledgement documentation for a sample of current employees and employees hired during the review period to determine that employees were required to sign a security acknowledgement form indicating their understanding of company security policies upon hire and annually thereafter for each employee sampled.	No exceptions noted.
3.03	New employee user access requests are documented and require the approval of a manager.	Inspected the new user access request documentation for a sample of new employees hired during the review period to determine that new employee user access requests were documented and required the approval of a manager for each new employee sampled.	No exceptions noted.
3.04	Systems administration personnel revoke system user accounts assigned to terminated employees upon notification of employee termination by HR or a department manager.	Inquired of the IT manager regarding the system access revocation process to determine that systems administration personnel revoked system user accounts assigned to terminated employees upon notification of employee termination by HR or a department manager.	No exceptions noted.
		Inspected the user account listing for a sample of in-scope system and the revocation requests for a sample of terminated employees during the review period to determine that systems administration personnel revoked system user accounts assigned to terminated employees upon notification of employee termination by HR or a department manager for each in-scope system and employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.05	Network user access privileges are reviewed on an annual basis to help ensure that accounts assigned to terminated employees are revoked.	Inspected the results of the most recent user access review for the network domain to determine that access privileges to the network domain were reviewed to ensure that accounts assigned to terminated employees were revoked during the review period.	No exceptions noted.
	Network Domain Authentication		
3.06	Network domain users are authenticated via a user account and password before being granted access to the network domain.	Inspected the authentication configurations and user account listings for the network domain to determine that network domain users were authenticated via a user account and password before being granted access to the network domain.	No exceptions noted.
3.07	The network domain is configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history requirements • Invalid password account lockout threshold	Inspected the network domain authentication configurations to determine that the network domain was configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history requirements • Invalid password account lockout threshold	No exceptions noted.
	Network Domain Access		
3.08	Administrative access privileges within the network domain are restricted to a user account accessible by the IT manager.	Inquired of the IT manager regarding administrative access to the network domain to determine that administrative access privileges within the network domain were restricted to a user account accessible by the IT manager.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the administrative user account listing for the network domain to determine that administrative access privileges within the network domain were restricted to a user account accessible by the IT manager.	No exceptions noted.
	Application Server Operating System Authentication		
3.09	Application server operating system users are authenticated via a user account and password before being granted access to the operating system.	Inspected the application server operating system authentication configurations and user account listings for a sample of production application servers to determine that the application server operating system users were authenticated via a user account and password before being granted access to the operating system for each server sampled.	No exceptions noted.
3.10	The application server operating system is configured to enforce the following user account and password requirements: • Minimum password length • Invalid password account lockout threshold • Complexity	Inspected the authentication configurations for a sample of production application servers to determine that the production application server operating system was configured to enforce the following user account and password requirements for each production application server sampled: • Minimum password length • Invalid password account lockout threshold • Complexity	No exceptions noted.
	Application Server Operating System Access		
3.11	Administrative access privileges within the application server operating system are restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	Inspected the administrator user account listings for a sample of production application servers to determine that administrative access privileges within the production application servers were restricted to user accounts accessible by persons holding the following positions for each production application server sampled: • Engineer • Third-party contractor	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Database Server Operating System Authentication		
3.12	Database server operating system users are authenticated via a user account and password before being granted access to the operating system.	Inspected the database server operating system authentication configurations and user account listings for a sample of production database servers to determine that the database server operating system users were authenticated via a user account and password before being granted access to the operating system for each production database server sampled.	No exceptions noted.
3.13	The database server operating system is configured to enforce user account and password requirements.	Inspected the authentication configurations for a sample of production database servers to determine that the production database server operating system was configured to enforce user account and password requirements for each production database server sampled.	No exceptions noted.
	Database Server Operating System Access		
3.14	Administrative access privileges within the database server operating system are restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractors (4)	Inspected the administrator user account listings for a sample of production database servers to determine that administrative access privileges within the production database servers were restricted to user accounts accessible by persons holding the following positions for each production database server sampled: • Engineer • Third-party contractors (4)	No exceptions noted.
	Database Authentication		
3.15	Database users are authenticated via a user account and password before being granted access to the production database.	Inspected the database authentication configurations for a sample of production databases to determine that database users were authenticated via a user account and password before being granted access to the production database for each production database.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.16	The production database is configured to enforce the following user account and password requirements: • Minimum length requirements • Password complexity • Password reuse	Inspected the authentication configurations for a sample of production databases to determine that production databases were configured to enforce the following user account and password requirements for each database sampled: • Minimum length requirements • Password complexity • Password reuse	No exceptions noted.
	Database Access		
3.17	Administrative access privileges within the database is restricted to a user accounts accessible by persons holding the following positions: • VP of engineering • Engineer • Third-party contractors (5)	Inspected the administrative user account listing for a sample of production databases to determine that administrative access privileges within each production database were restricted to user accounts accessible by persons holding the following positions for each database sampled: • VP of engineering • Engineer • Third-party contractors (5)	No exceptions noted.
	AWS Management Console Authentication		
3.18	AWS management console users are authenticated via a user account and password before being granted access to the AWS management console users.	Inspected the AWS management console authentication configurations and the AWS user account listing to determine that AWS management console users were authenticated via a user account and password before being granted access to the AWS management console.	No exceptions noted.
3.19	The AWS management console is configured to enforce the following user account and password requirements: • Minimum password length • Password complexity • Password age • Minimum password history	Inspected the AWS management console authentication configurations to determine that the AWS management console was configured to enforce the following user account and password requirements: • Minimum password length • Password complexity • Password age • Minimum password history	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	AWS Management Console Access		
3.20	Administrative access privileges within the AWS management console are restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer • Third-party contractor	Inspected the administrator access listing for the AWS management console to determine that administrative access privileges within the AWS management console were restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer • Third-party contractor	No exceptions noted.
	Noosh Application Authentication		
3.21	Application users are required to authenticate via a user account and password before being granted access to the application.	Inspected the application authentication configurations and the application administrator user account listing to determine that application users were authenticated via a user account and password before being granted access to the application.	No exceptions noted.
3.22	The application is configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history requirements • Invalid password account lockout threshold	Inspected the application password configurations to determine that the application was configured to enforce the following user account and password controls: • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history requirements • Invalid password account lockout threshold	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Noosh Application Access		
3.23	Administrative access privileges within the application are restricted to user accounts accessible by persons holding the following positions: • VP of engineering • VP of customer success • Release manager • QA manager	Inspected the application administrator user account listing to determine that administrative access privileges within the application were restricted to user accounts accessible by persons holding the following positions: • VP of engineering • VP of customer success • Release manager • QA manager	No exceptions noted.

DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Firewall System		
4.01	A firewall system is in place and configured to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the firewall system configurations to determine that a firewall system was in place and configured to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
4.02	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the firewall system configurations to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
4.03	NAT functionality of the firewall system is utilized to translate internal IP addresses to publicly routable IP addresses.	Inspected the firewall system configurations to determine that NAT functionality of the firewall system was utilized to translate internal IP addresses to publicly routable IP addresses.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.04	Firewall users are authenticated via a user account and password prior being granted access to the firewall system.	Inspected the firewall system authentication configurations to determine that firewall users were authenticated via a user account and password prior being granted access to the firewall system.	No exceptions noted.
4.05	Administrative access privileges within the firewall system are restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	Inquired of the engineer regarding administrative access privileges to determine that administrative access privileges within the firewall system were restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	No exceptions noted.
		Inspected the firewall administrator listing to determine that administrative access privileges within the firewall system were restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	No exceptions noted.
	Security Groups		
4.06	EC2 security groups are in place and configured to filter unauthorized inbound network traffic unless explicitly authorized by a security group rule.	Inspected the security group configurations to determine that EC2 security groups were in place and configured to filter unauthorized network traffic unless explicitly authorized by a security group rule.	No exceptions noted.
4.07	AWS management console users are authenticated via a user account and password before prior granted access to the AWS management console users.	Inspected the AWS management console authentication configurations to determine that AWS management console users were authenticated via a user account and password prior being granted access to the AWS management console.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.08	The ability to modify EC2 security groups within the AWS management console is restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer • Third-party contractor	Inspected the AWS management console administrator listing to determine that the ability to modify EC2 security groups within the AWS management console was restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Engineer • Third-party contractor	No exceptions noted.
	Remote Access		
4.09	Remote access to the production environment is secured via encrypted VPN systems and require a user account and password.	Inquired of the engineer regarding remote access to the production environment to determine that remote access to the production environment was secured via encrypted VPN systems and required a user account and password.	No exceptions noted.
		Inspected the VPN systems configurations to determine that remote access to the production environment was secured via encrypted VPN systems and required a user account and password.	No exceptions noted.
4.10	Administrative access privileges within the VPN systems are restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	Inquired of the engineer regarding administrative access privileges to the VPN systems to determine that administrative access privileges within the VPN systems were restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	No exceptions noted.
		Inspected the VPN administrator listings to determine that administrative access privileges within the VPN systems were restricted to user accounts accessible by persons holding the following positions: • Engineer • Third-party contractor	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.11	Customer web communication sessions are secured with TLS encryption.	Inspected the website certificate for the production Noosh website to determine that customer web communication sessions were secured with TLS encryption.	No exceptions noted.

Application Change Control

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that unauthorized changes are not made to production application systems.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Documented change control policies and procedures are in place to guide personnel in processes that include, but are not limited to, the following: • Application development and release process • QA process • Version control	Inspected policy and procedure documentation to determine that documented change control policies and procedures were in place to guide personnel in processes that included the following: • Application development and release process • QA process • Version control	No exceptions noted.
5.02	A sprint planning meeting is held on a monthly basis to plan and prioritize upcoming development projects.	Inquired of the QA manager regarding sprint planning meetings to determine that spring sprint planning meetings were held on a monthly basis to plan and prioritize upcoming development projects.	No exceptions noted.
		Inspected the sprint planning meeting invite, sprint backlogs, and the sprint plan for a sample of months during the review period to determine that sprint planning meetings were held for each month sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.03	A change management tracking system is utilized to centrally maintain, manage, and monitor change control activities.	Inspected the change management system and the change request ticket for a sample of application changes implemented to production during the review period to determine that a change management tracking system was utilized to centrally maintain, manage, and monitor change control activities for each change sampled.	No exceptions noted.
5.04	Application development and testing efforts are performed in development and test environments that are logically separated from the production environment.	Inquired of the release manager regarding application development and testing procedures to determine that application development and testing efforts were performed in development and test environments that were logically separated from the production environment.	No exceptions noted.
		Inspected the development and production environment configurations to determine that application development and testing efforts were performed in development and test environments that were logically separated from the production environment.	No exceptions noted.
5.05	QA personnel perform functional testing for application changes prior to implementation.	Inquired of the release manager regarding testing to determine that QA personnel performed functional testing for application changes prior to implementation.	No exceptions noted.
		Inspected the change documentation for a sample of application changes implemented to production during the review period to determine that QA personnel performed functional testing prior to implementation for each change sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.06	IT personnel approve application change requests prior to implementation.	Inspected the change documentation for a sample of application changes implemented to production during the review period to determine that IT personnel approved application change requests prior to implementation for each change sampled.	No exceptions noted.
5.07	Release implementation team meetings are held on a weekly basis to prioritize and approve upcoming releases.	Inquired of the QA manager regarding release implementation team meetings to determine that release implementation team meetings were held on a weekly basis to prioritize and approve upcoming releases.	No exceptions noted.
		Inspected the recurring release implementation team meeting invite and meeting minutes for a sample of weeks during the review period to determine that that release implementation team meetings were held to prioritize and approve upcoming releases for each week sampled.	No exceptions noted.
5.08	Version control software is utilized to control access to source code and provide roll back capabilities for application changes.	Inspected the version control software configurations to determine that version control software was utilized to control access to source code and provide roll back capabilities for application changes.	No exceptions noted.
5.09	The ability to modify development source code in the version control software is restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Release manager • Engineers (3) • Developers (14)	Inspected the version control software user access permissions to determine that the ability to modify source code in the version control software was restricted to user accounts accessible by persons holding the following positions: • VP of engineering • Release manager • Engineers (3) • Developers (14)	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.10	Administrative access privileges within the version control software are restricted to user accounts accessible by persons holding the following positions: • Release manager • Engineers (2)	Inspected the version control software administrative access permissions to determine that the administrative access privileges within the version control software were restricted to user accounts accessible by persons holding the following positions: • Release manager • Engineers (2)	No exceptions noted.
5.11	The ability to implement application changes to the production environment is restricted to user accounts accessible by the following positions: • VP of engineering • Engineer	Inquired of the engineer regarding the ability to implement application changes to production to determine that the ability to implement application changes to production was restricted to user accounts accessible by the following positions: • VP of engineering • Engineer	No exceptions noted.
		Inspected user account permissions to the code deployment tool to determine that the ability to implement application changes to production was restricted to user accounts accessible by the following positions: • VP of engineering • Engineer	No exceptions noted.
5.12	The version control software is configured to restrict users from merging code without peer approval, thus preventing any one user from both developing and implementing code to the production environment.	Inspected the protected branch configurations within the version control software to determine that the version control software was configured to restrict users from merging code without peer approval, thus preventing any one user from both developing and implementing code to the production environment.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.13	A version monitoring script to is utilized to monitor for changes to the production environment and send daily e-mail notifications to persons holding the following positions: • VP of engineering • IT manager • Engineer • Third-party contractor	Inquired of the engineer regarding the version monitoring script to determine that a version monitoring script was utilized to monitor for changes to the production environment and send daily e-mail notifications.	No exceptions noted.
		Inspected the version monitoring script configurations and an example e-mail notification generated during the review period to determine that a version monitoring script was utilized to monitor for changes to the production environment and send daily e-mail notifications to persons holding the following positions: • VP of engineering • IT manager • Engineer • Third-party contractor	No exceptions noted.