System and Organization Controls (SOC) for Service Organizations

SOC 2

For

AllVoices Platform

A Type II Report on AllVoices' Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security

December 15, 2021, to June 30, 2022

Report of Independent Service Auditors issued by AssurancePoint, LLC

Proprietary and Confidential

This report is intended solely for use by the management of AllVoices Holding Co., user entities of AllVoices Holding Co.’s services, and other parties who have sufficient knowledge and understanding of AllVoices Holding Co.’s services covered by this report (each referred to herein as a “specified user”).

If report recipient is not a 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 AllVoices Holding Co. or AssurancePoint, LLC as a result of such access. Further, AllVoices Holding Co. and AssurancePoint, LLC assume no duties or obligations to any non-specified user who obtains this report and/or has access to it.

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

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To AllVoices Holding Co.:

Scope

We have examined AllVoices Holding Co.'s ("AllVoices" or the "service organization") accompanying description of its AllVoices Platform system, in Section 3, throughout the period December 15, 2021, to June 30, 2022, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 15, 2021, to June 30, 2022, to provide reasonable assurance that AllVoices' service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

AllVoices uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AllVoices, to achieve AllVoices' service commitments and system requirements based on the applicable trust services criteria. The description presents AllVoices' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AllVoices' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 AllVoices, to achieve AllVoices' service commitments and system requirements based on the applicable trust services criteria. The description presents AllVoices' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AllVoices' 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

AllVoices 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 AllVoices' service commitments and system requirements were achieved. AllVoices has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. AllVoices 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 Auditor's 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; and
- 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 Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

a. the description presents the AllVoices Platform system that was designed and implemented throughout the period December 15, 2021, to June 30, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period December 15, 2021, to June 30, 2022, to provide reasonable assurance that AllVoices' 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 the user entities applied the complementary controls assumed in the design of AllVoices' controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period December 15, 2021, to June 30, 2022, to provide reasonable assurance that AllVoices' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and user entity controls assumed in the design of AllVoices' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of AllVoices; user entities of AllVoices Platform system during some or all of the period December 15, 2021, to June 30, 2022, business partners of AllVoices subject to risks arising from interactions with the AllVoices Platform system, 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; and
- 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.

AssurancePoint, LLC

Atlanta, Georgia
July 29, 2022

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

We have prepared the accompanying description of the AllVoices Platform system, in Section 3, throughout the period December 15, 2021, to June 30, 2022, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the AllVoices Platform system that may be useful when assessing the risks arising from interactions with AllVoices' system, particularly information about system controls that AllVoices 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 ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

AllVoices uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AllVoices, to achieve AllVoices' service commitments and system requirements based on the applicable trust services criteria. The description presents AllVoices' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AllVoices' controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents the AllVoices Platform system that was designed and implemented throughout the period December 15, 2021, to June 30, 2022, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period December 15, 2021, to June 30, 2022, to provide reasonable assurance that AllVoices' 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 organizations and the user entities applied the complementary controls assumed in the design of AllVoices' controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period December 15, 2021, to June 30, 2022, to provide reasonable assurance that AllVoices' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of AllVoices' controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

AllVoices was founded to solve the need for a comprehensive and effective employee feedback system. Management of AllVoices recognized that existing options for employees to communicate important or sensitive issues to employers were ineffective, intimidating, outdated, and rarely used. The AllVoices Platform (Platform) was created to build a better, more inclusive, and vibrant workplace allowing companies to ask for, accept, analyze, and act upon employee feedback of all kinds.

Description of Services Provided

AllVoices' Platform is an anonymous reporting and feedback platform built for the employee and the employer. The Platform provides a reporting tool, feedback platform, and case management system for the workplace. Employees use the system to report issues and share feedback anonymously directly to company leadership providing transparency to management regarding internal operations and issues. Company administrators can input cases and track and manage them within the system from beginning to resolution.

Principal Service Commitments and System Requirements

AllVoices designs its processes and procedures related to the AllVoices Platform to meet its objectives for its services. Those objectives are based on the service commitments that AllVoices makes to user entities, the laws and regulations that govern the provision of the AllVoices Platform services, and the financial, operational, and compliance requirements that AllVoices has established for the services.

Security commitments to user entities are documented and communicated online through the Privacy Notice. The principal security commitments are standardized and include, but are not limited to, the following:

- The use of physical, organizational, and technical safeguards that are designed to aid in maintaining the integrity and security of information that we collect

AllVoices establishes operational requirements that support the achievement of the principal service commitments. System requirements include the use of encryption technologies to protect system user data both at rest and in transit, system monitoring controls to detect security threats, anomalies, unusual activity, or performance issues, incident response procedures, logical access control standards, and change management standards.

Such requirements are communicated in AllVoices' system policies and contracts with customers. Information security and privacy policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the AllVoices Platform.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Components of the System

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

The AllVoices platform is a software-as-a-service (SaaS) cloud-based system. The primary components of the system are built on top of AWS, using the following services:

Primary Infrastructure	
Infrastructure Component	**Business Function Description**
Amazon CloudFront	CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and application programming interfaces (APIs) to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.
Amazon CloudTrail	CloudTrail provides customers the ability to log, continuously monitor, and retain account activity related to actions across their AWS infrastructure.
Amazon CloudWatch	CloudWatch provides customers with data and actionable insights to monitor their applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.
Amazon Elastic Container Registry (ECR)	ECR is a fully managed container registry that makes it easy to store, manage, share, and deploy container images and artifacts.
Amazon ElastiCache	ElastiCache allows the user to seamlessly set up, run, and scale open-source compatible in-memory data stores in the cloud.
Amazon GuardDuty	GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon S3.
Amazon Inspector	Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.
Amazon Relational Database Service (RDS)	RDS is used to set up, operate, and scale relational databases in the cloud.
Amazon Route 53	Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.
Amazon Simple Email Service (SES)	SES is an e-mail service that enables developers to send mail from within any application.
Amazon Simple Queue Service (SQS)	SQS is a fully managed message queuing service that enables the user to decouple and scale microservices, distributed systems, and serverless applications.
Amazon Simple Storage Service (S3)	S3 is virtual storage used to store object data. Amazon S3 is also used to automatically replicate data across AWS regions.

Primary Infrastructure	
Infrastructure Component	**Business Function Description**
AWS Elastic Compute Cloud (EC2)	EC2 provides scalable computing capacity in the AWS Cloud.
AWS Elastic Kubernetes Service (EKS)	EKS managed node groups automate the provisioning and life cycle management of nodes (Amazon EC2 instances) for Amazon EKS Kubernetes clusters.
AWS Elastic Load Balancers	Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, Lambda functions, and virtual appliances. It can handle the varying load of application traffic in a single Availability Zone or across multiple Availability Zones.
AWS Key Management Service (KMS)	KMS is used to create and manage cryptographic keys and control their use across a wide range of AWS services and in customer applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect customer keys.
AWS Simple Notification Service (SNS)	SNS is a fully managed messaging service for both application-to application (A2A) and application-to-person (A2P) communication.
AWS Systems Manager	Systems Manager is the operations hub for AWS. Systems Manager provides a unified user interface so the user can track and resolve operational issues across AWS applications and resources from a central place.
AWS Virtual Private Cloud (VPC)	VPC is a service that lets customers launch AWS resources in a logically isolated virtual network that the user defines. Customers have complete control over their virtual networking environment, including selection of their IP address range, creation of subnets, and configuration of route tables and network gateways.

Additionally, the following secondary systems and software are used to support the system:

Additional Vendor Provided Services	
System/Software	**Business Function Description**
GitHub	GitHub provides hosting for software development version control using Git. GitHub provides access control and several other collaboration features such as bug tracking, feature requests, task management, and wikis for projects.
Jira	Jira is an internal ticketing system used to manage and track projects and tasks.
Terraform	Terraform is an open-source infrastructure-as-code software tool that provides a consistent command line interface (CLI) workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.
Trello	Trello is a collaboration tool that organizes projects into boards. In one glance, Trello tells the user what is being worked on, who is working on what, and where something is in a process.
Twilio	Twilio allows software developers to programmatically make and receive phone calls, send and receive text messages, and perform other communication functions using its web service APIs.

People

The control framework that supports AllVoices organizational environment starts with its executive team. The following are key roles involved in control implementation and maintenance:

- Chief Executive Officer (CEO)
- Chief Technology Officer (CTO)
- Vice President (VP) of Engineering

Responsibility for AllVoices' information security resides with the Chief Technology Officer. In addition to the overall governance provided by the executive team, the following teams play a key role in the execution of controls:

- Engineering: The engineering team is responsible for software development.
- Incident Response: The incident response team is responsible for the detection, containment, and eradication of incidents in an organized, timely, and cost-effective manner.

Data

Within the Platform, service data (or customer data) consists of (mostly anonymous) employee reports and feedback, as well as administrative information for each case. In some cases, the customer opts to add additional employee information into the system such as employee name, job title, e-mail, and more.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer Data	Customer provided data	Confidential
Personal Identifiable Information	Customer provided data	Confidential

Procedures

Access, Authentication and Network

Documented access control policies and procedures have been implemented to help ensure access to information systems is restricted to authorized personnel. Management has documented and maintains an access control matrix to define the appropriate level of access permissions authorized for certain personnel and roles within the entity. Management further maintains an inventory of information assets through the internal security and compliance system integrations.

Access to production resources is controlled through role-based access permissions and group privileges within the AWS cloud console and within supporting secondary systems. Only user groups with pre-established trusted roles attached can access resources within the production account. Network security groups are used to filter network traffic to authorized sources and protocols. A web application firewall (WAF) is also in place to filter Internet traffic to the production application to authorized sources. Multifactor authentication is configured for personnel to access production compute resources, data stores, or to perform administrative functions within the production cloud hosted environment. Supporting infrastructure and software, such as the source code repository and the internal directory and collaboration service, are also configured to enforce multifactor authentication. Access to administer production resources are restricted to user accounts accessible by authorized personnel. Native system root accounts are not used for administering resources or provisioning access privileges. Knowledge of root account credentials is restricted to authorized personnel. Databases housing sensitive data are configured to be encrypted to help prevent unauthorized disclosure of sensitive information.

The production application is further configured to authenticate users via predetermined hard-coded authentication policies, which include minimum password lengths, password complexity, and invalid login attempt thresholds.

Access Requests and Access Revocation

AllVoices has implemented role-based security to limit and control access within AllVoices' production environment. New access to AllVoices' systems is provisioned through notifications of employment to engineering personnel from the HR department. Notifications include job descriptions and start dates which indicate when access privileges should be provisioned. Engineering personnel utilize the documented access matrix to guide the access privileges to provision the new employee.

User access reviews are conducted on a quarterly basis to help validate existing access to production systems and supporting applications is authorized and commensurate with the users' job function. When an internal user is terminated, engineering personnel are required to revoke the user's access to internal systems within one business day of the separation date.

Once onboarded, customers have the ability to set up an account using their e-mail address and creating a password. The administrator of the account is then responsible for adding, editing, or remove team members to their company's account in the AllVoices platform.

Data Transmissions

AllVoices maintains a Cryptography Policy to support the secure encryption and decryption of application transmissions. User application sessions utilize HTTPS/TLS transmission protocols to encrypt data transmitted over the Internet.

Anti-malware

Standard base images are utilized to enforce configurations and security requirements over production infrastructure. Anti-malware software is also deployed on laptops of employees with access to production infrastructure. The security and compliance application monitors employee workstations and notifies management if employee laptops are implemented that are not configured with antivirus protections.

Change Management

AllVoices has a formalized change management process documented in its Change Management Policy. Specifically, AllVoices has developed policies and procedures governing the system development life cycle, including documented processes for tracking, testing, approving, and validating changes. Both code and infrastructure changes are recorded in a ticketing system. The production environment is segregated from the staging environment to allow for changes to be developed and tested outside of production. Production data is not used in the development and testing environments.

Production application code changes undergo automated testing prior to changes being merged to production. Following testing, an independent engineer reviews and approves these changes prior to deploying into production. System users who make changes in the development system are unable to deploy their changes into production without independent review and approval.

System Monitoring

AllVoices uses detection and monitoring software to collect data from servers and endpoints and to detect potential security threats or unusual system activity due to changes to configurations, susceptibility to vulnerabilities, and anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives. Alerting software compiles logs from the monitoring tools and notifies the incident response team of potential security events. The engineering team tracks identified events through resolution.

AllVoices has also implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.

Incident Response

Management has established an Incident Response Plan outlining the process of identifying, prioritizing, communicating, assigning, and tracking incidents. Identified security events and issues are triaged and tracked to resolution in accordance with the Incident Response Plan. Incidents are tracked via a ticketing a system and/or incident investigation forms. “Lessons learned” are documented by the Incident Response team within the incident ticket after each incident in an effort to identify root cause of the incident and prevent similar issues from recurring.

Significant Changes During the Review Period

There were no significant changes that are likely to affect report users’ understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at AllVoices, and the types of controls expected to be implemented at AWS to achieve AllVoices’ service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for ensuring access to its facilities and the physical information assets hosted within its facilities is restricted to authorized personnel.	CC6.4
AWS is responsible for ensuring physical media containing production data is securely sanitized or destroyed prior to being removed from its data center or protected areas within its data center facilities.	CC6.5

Control Environment

The control environment at AllVoices 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 executive management & the board of directors and operations management.

Integrity and Ethical Values

The AllVoices control environment reflects the philosophy of senior management concerning the importance of integrity and ethical values. AllVoices management understands that leadership sets the tone from the top, where the actions of, and decisions by, management at all levels of the organization establish the basis for acceptable behavior. AllVoices has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.

Executive Management & Board of Directors Oversight

The board of directors is composed of both senior management and external board members who are independent from AllVoices operations. On a quarterly basis, senior management meets with the board of directors to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.

Organizational Structure and Assignment of Authority and Responsibility

The organizational structure of AllVoices is found in the organizational chart posted in a shared drive on the company network. Management maintains the organizational chart to clearly identify positions of authority and the lines of communication. The organizational chart is available for reference by personnel as needed. Policies are further in place to assign specific roles to personnel throughout the organization with respect to the development, performance, and oversight of the entity's information security program.

Commitment to Competence

Prior to employee onboarding, hiring managers evaluate whether candidates are qualified to perform the required job duties. Employment candidates pass through evaluative interviews against predetermined job requirements. If a candidate is successful in the screening process, a reference check is conducted prior to the start date, and a background check is also performed for US-based new hires within 60 days of hire.

Formal hiring procedures are followed for new hires. The onboarding process begins when a candidate accepts and signs and offer letter. During orientation, AllVoices works to ensure new hires are aware of their responsibilities and obligations to protect AllVoices and customer information. Specifically, internal personnel (new employees and contractors who have access to production systems) review the Code of Conduct, Access Control Policy, Data Management Policy, Incident Response Plan, and Information Security Policy and formally acknowledge them within 30 days of hire. Failure to comply with these agreed upon policies may result in disciplinary actions in proportion to their violation decided by management.

Personnel complete information security training programs within 60 days of hire and annually thereafter to help them understand their obligations and responsibilities related to security. Management evaluates the performance of personnel through a formal, annual performance evaluation. This process assesses the performance and competence of individuals with respect to their job role and their compliance with company policies and procedures.

Accountability

AllVoices has a formal process for documenting and reporting issues of noncompliance with policies and procedures. Events and behaviors that do not meet expectations as outlined in policies are documented and disciplinary action is taken upon the personnel responsible for the infraction. Each of the company policies and procedures, including the code of conduct, contain a clause for sanctions regarding noncompliance with the policies outlined therein.

Risk Assessment

Objective Setting

Management formally specifies entity-wide objectives designed to help achieve the service commitments made to users, comply with laws and regulations, and to achieve the operational and strategic goals of the organization. The entity's objectives are incorporated and documented within each of the company policies to serve as the purpose for the origination of the policy and underlying procedures.

Risk Identification and Analysis

AllVoices has established a risk assessment and management program that includes the identification, evaluation, communication, and mitigation of risks relating to the company operations, relevant internal and external threats, safeguarding of informational assets, product development, and fraud. The risk assessment and management program is reviewed and approved annually within the Risk Management Policy.

On an annual basis, a formal risk assessment is performed over the company and platform services. This assessment includes the identification of relevant internal and external threats related to security and fraud, an analysis of risks associated with those threats, a determination of appropriate risk mitigation strategies, and the development or modification or controls consistent with the Risk Management Policy.

Identified risks are analyzed based on the impact if the risk were to materialize and likelihood of the risk materializing. Risks are assigned a score of 1-3 within each category then are multiplied together to obtain a risk severity score. Risks are ranked and prioritized for mitigation based on the risk severity score.

Risk Mitigation

As a result of the annual risk assessment, action plans are documented in a risk register and tracked to address identified risks that are deemed unacceptable. Owners are assigned responsibility for the mitigating tasks and projected due dates are documented. Management takes a prioritized approach to responding to identified risks based on the risk score determined through the impact and likelihood analysis. Management has further obtained a cyber risk insurance policy to minimize the financial impact of a cybersecurity loss event.

Management also maintains a formal vendor risk management program. Prior to engaging a new vendor, an assessment of risks associated with the vendor is performed to validate whether potential third-party service providers meet compliance requirements as defined in the Vendor Management Policy. AllVoices management maintains an inventory of service providers within its security and compliance platform. Vendors are initially provided a risk classification (low, medium, high) based on the perceived risk associated with the vendor. High risk vendors are further evaluated annually by obtaining a third-party compliance report or a completed security questionnaire.

Trust Services Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out to sufficiently mitigate risks to acceptable levels. Control activities serve as mechanisms for managing the achievement of AllVoices' objectives and service commitments.

Selection and Development of Control Activities

The security category and the applicable trust services criteria were used to evaluate the suitability of the design and operating effectiveness of controls stated within the description. Security criteria and related control activities designed, implemented, and operated to meet them are included in Section 4 of this report. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of AllVoices' description of the system.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security category are applicable to the AllVoices Platform system.

INFORMATION AND COMMUNICATION SYSTEMS

To help AllVoices achieve its goals, management is committed to using quality information and effective communication channels both with employees and customers. Descriptions of the system and its boundaries are available to both internal and external users on the website and via the company privacy policy.

Internal Communications

Management publishes policies and procedures, including internal security policies and procedures, on the policy and procedure portal within its security and compliance platform. Information security policies outline the roles and responsibilities for personnel with responsibility for the security of the system. The chief technology officer is responsible for the design, implementation, and management of the security policies. The policy owners are responsible for an annual review of company policies and procedures.

AllVoices has established a confidential reporting process available to internal and external users. Management monitors customer and internal complaints reported via the confidential reporting process and responds in accordance with the Incident Response Plan.

External Communications

AllVoices communicates security commitments and expectations, changes to roles and responsibilities, and changes impacting the security of the system to customers. Customers may also contact AllVoices through the website to report incidents, complaints, and failures on issues related to security. Internal or customer initiated incident tickets are assigned to the appropriate team or individual and are prioritized based on policy and business impact. An internal tracking system is used to document issues through resolution.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

To evaluate the effectiveness of controls management utilizes a security and compliance monitoring tool to continually assess controls and to alert when controls are identified as out of compliance with predetermined baselines. Security personnel evaluate the results and resolve deficiencies in accordance with the event and incident management policies and procedures. In addition, management performs additional monitoring activities, including quarterly access reviews, monthly vulnerability scanning, an annual penetration test, and an annual review of third parties.

AllVoices uses logging and monitoring software to collect data from servers and endpoints, detect potential security threats, and unusual system activity. Once detected, the Incident Response team uses alerting software to notify impacted teams of potential security events. The Engineering team tracks identified events through resolution.

Separate Evaluations

Management performs periodic internal evaluations and contracts third parties periodically to determine the presence of the required components of internal control and to assess if those components are functioning as designed. System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes needed, as a result of the review, are tracked to remediation. Security personnel execute vulnerability scans on production systems weekly. Identified vulnerabilities are tracked through the security and compliance platform in accordance with predefined SLAs.

A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Results are reviewed and high priority findings are tracked through resolution.

Subservice Organization Monitoring

AllVoices' management monitors subservice organizations annually by obtaining and reviewing the current SOC reports for its subservice organizations for controls expected to be implemented by those service providers to support the achievement of AllVoices' service commitments and system requirements.

Evaluating and Communicating Deficiencies

Risk assessments and other periodic internal and external assessments are designed to help identify deficiencies in the design and/or operation of control activities. Results from external assessments are communicated to senior management. Senior management meets with the board of directors quarterly to review business objectives, company initiatives, resource needs, and risk management activities, including results from external assessments. This level of visibility allows both senior management and the board of directors to maintain oversight of the deficiency and help ensure the correct response is enacted by the control owners.

System Incidents Identified During the Review Period

No incidents to the AllVoices system during the review period of this report were identified or reported that could have impaired the achievement of our service commitments and system requirements.

Complementary Controls at User Entities

The following complementary user entities controls should be implemented by user entities to provide additional assurance that the applicable trust 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

#	Complementary User Entity Control	Related Applicable Trust Criteria
1.	User entities are responsible for implementing controls to ensure only authorized individuals are granted access.	CC6.1, CC6.2, CC6.3
2.	User entities are responsible for implementing controls to ensure access for terminated users is removed timely.	CC6.1, CC6.2, CC6.3
3.	User entities are responsible for implementing controls to ensure user accounts and access permissions are periodically reviewed.	CC6.2, CC6.3

Section 4

Trust Services Criteria, Related Controls, and Tests of Controls

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope

This report relates to the AllVoices Platform system provided by AllVoices and the relevant controls designed and operated during the period December 15, 2021, through June 30, 2022, specified by management of AllVoices that are believed by management to be relevant to user entities of this report. The scope of AssurancePoint's testing was restricted to the Trust Services Criteria selected by management of AllVoices and the boundaries of the AllVoices Platform system defined in Section 3. AssurancePoint's examination was performed in accordance with American Institute of Certified Public Accountants ("AICPA") Statements on Standards for Attestation Engagements, specifically AT-C section 105 *"Concepts Common to All Attestation Engagements"* and AT-C section 205, *"Examination Engagements"*.

Tests of Operating Effectiveness

The tests applied by AssurancePoint to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting tests of controls, AssurancePoint 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
- The degree to which the control relies on the effectiveness of other controls
- Whether the control is performed manually or is automated

The types of tests performed with respect to the operating effectiveness of the control activities detailed in this section are 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. Inquiry alone is not deemed sufficient to evidence operating effectiveness of a control activity and is always accompanied by a testing method that provides greater levels of assurance.
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.).
Re-performance	Re-performed procedures or controls that were originally performed by the service organization to independently validate conclusions or results.

Sampling

Consistent with AICPA authoritative literature, AssurancePoint utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the control population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. AssurancePoint, 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.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Results of Tests

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

Testing Matrices

Security Category

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.0: Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	AllVoices has established a Code of Conduct outlining ethical expectations, behavioral standards, and ramifications for noncompliance. The Code of Conduct is communicated to personnel via the security and compliance application.	Inspected the Code of Conduct within the security and compliance application to determine that AllVoices established a Code of Conduct which outlined the ethical expectations, behavioral standards, and ramifications for noncompliance and that the document was communicated to personnel via the security and compliance application.	No exceptions noted.
CC1.1.2	Personnel are required to acknowledge the Code of Conduct and the company information security policies within 30 days of hire.	Inspected the policy and procedure acknowledgement records for a sample of employees hired during the review period to determine that each employee sampled acknowledged the Code of Conduct and the company information security policies within 30 days of hire.	No exceptions noted.
CC1.1.3	Background checks are performed for US-based new hires within 60 days of hire.	Inspected the background check records for a sample of employees hired during the review period to determine that each employee sampled had a completed background check on file within 60 days of hire.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors includes senior management and external members who are independent from AllVoices operations.	Inspected the meeting minutes for a sample board of directors meeting to determine that the board of directors included senior management and external members who were independent from AllVoices operations.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC1.2.2	Senior management meets with the board of directors quarterly to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	Inspected the board of directors meeting minutes for a sample of quarters during the review period to determine that senior management met with the board of directors for each quarter during the review period sampled to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	No exceptions noted.
CC1.2.3	An Information Security Roles and Responsibilities Policy is implemented which outlines the roles and responsibilities of personnel with respect to the security of the system.	Inspected the Information Security Roles and Responsibilities Policy to determine that the policy was implemented and outlined the roles and responsibilities of personnel with respect to the security of the system.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Management maintains a formal organizational chart to clearly identify positions of authority and lines of communication. The organizational chart is published in a shared workspace for reference by personnel.	Inspected the organizational chart to determine that management maintained a formal organizational chart to clearly identify positions of authority and lines of communication.	No exceptions noted.
		Inspected the shared workspace in the company network containing the organizational chart k to determine that the organizational chart was published in a shared workspace for reference by personnel.	No exceptions noted.
CC1.3.2	An Information Security Roles and Responsibilities Policy is implemented which outlines the roles and responsibilities of personnel with respect to the security of the system.	Inspected the Information Security Roles and Responsibilities Policy to determine that the policy was implemented and outlined the roles and responsibilities of personnel with respect to the security of the system.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.3.3	Personnel responsible for pursuit of company objectives through organization's policies and procedures are documented as owners within the policies and procedures. Policy owners are required to review and approve their owned policies and procedures on at least an annual basis.	Inspected a sample of the company policies and procedures to determine that personnel responsible for the design, implementation, and management of the policies and procedures were documented as owners within each policy and procedure sampled and that the owners reviewed the sampled policies and procedures within the 12 months preceding the end of the review period.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Reference checks are performed on new hires before the hire's start date.	Inspected the new hire checklist for a sample of employees hired during the review period to determine that reference checks were performed for each new hire selected prior to the employee's start date.	No exceptions noted.
CC1.4.2	Hiring managers screen new hires to assess their qualifications, experience, and competency to fulfill the position responsibilities.	Inspected interview meeting invites for a sample of employees hired during the review period to determine that hiring managers screened each hire to assess their qualifications, experience, and competency to fulfill the position responsibilities.	No exceptions noted.
CC1.4.3	Personnel complete an information security training program within 60 days of hire and on an annual basis thereafter to help them understand their obligations and responsibilities related to security.	Inspected the security awareness training records for a sample of employees hired during the review period to determine that each employee sampled completed an information security training program within 60 days of hire.	No exceptions noted.
		Inspected the security awareness training records for a sample of existing employees to determine that each employee sampled had completed a security awareness training program within the 12 months preceding the end of the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.4.4	Personnel are required to acknowledge the Code of Conduct and the company information security policies within 30 days of hire.	Inspected the policy and procedure acknowledgement records for a sample of employees hired during the review period to determine that each employee sampled acknowledged the Code of Conduct and the company information security policies within 30 days of hire.	No exceptions noted.
CC1.4.5	Management evaluates the performance of personnel through a formal performance evaluation on an annual basis.	Inspected completed performance evaluations for a sample of employees with tenure greater than one year to determine that each employee sampled had been evaluated by management through a formal performance evaluation within the 12 months preceding the end of the review period.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Management evaluates the performance of personnel through a formal performance evaluation on an annual basis.	Inspected completed performance evaluations for a sample of employees with tenure greater than one year to determine that each employee sampled had been evaluated by management through a formal performance evaluation within the 12 months preceding the end of the review period.	No exceptions noted.
CC1.5.2	Personnel are required to acknowledge the Code of Conduct, Access Control Policy, Data Management Policy, Incident Response Plan, and Information Security Policy within 30 days of hire.	Inspected policy acknowledgements for a sample of employees hired during the review period to determine that each employee sampled acknowledged the Code of Conduct, Access Control Policy, Data Management Policy, Incident Response Plan, and Information Security Policy within 30 days of hire.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC1.5.3	An employee sanction procedure is in place and documented within the employee code of conduct communicating that employees may be disciplined by management for noncompliance with a policy and/or procedure.	Inspected the code of conduct and determined that it included an employee sanction procedure which communicated that employees may be disciplined by management for noncompliance with a policy and/or procedure.	No exceptions noted.
CC2.0: Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	AllVoices uses a compliance monitoring tool to perform a continual assessment over internal controls. The tool communicates deficiencies to management in real-time through in application alerts.	Inspected the compliance monitoring tool monitoring dashboards to determine that the tool performed a continuous assessment over the entity's internal controls and communicated deficiencies to management in real-time through in application alerts.	No exceptions noted.
CC2.1.2	A risk assessment which includes the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats is performed on an annual basis.	Inspected the completed annual risk assessment to determined that a risk assessment which included the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats was performed within the 12 months preceding the end of the review period.	No exceptions noted.
CC2.1.3	Vulnerability scans are executed weekly on production systems. Identified vulnerabilities are tracked through the security and compliance platform in accordance with predefined SLAs.	Inquired of the VP of engineering regarding vulnerability scans to determine that vulnerability scans were executed on a weekly basis and identified vulnerabilities were tracked through the security and compliance platform.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
		Inspected the vulnerability scanning application configurations and tracking dashboards within the security and compliance monitoring tool to determine that vulnerability scans were executed weekly on production systems and that identified vulnerabilities were tracked through the security and compliance platform in accordance with predefined SLAs.	No exceptions noted.
CC2.1.4	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Results are reviewed and high priority findings are tracked through resolution.	Inspected the most recent penetration test report to determine that a third part was engaged to perform an application penetration test during the 12 months preceding the end of the review period.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Company policies are prefaced by the organization's objective the policy is intended to achieve. Policies are communicated to personnel via the security and compliance application.	Inspected a sample of company policies and procedures to determine that each policy sampled was prefaced by an organizational objective which the policy was intended to achieve.	No exceptions noted.
		Inspected the policy and procedure module within the security and compliance platform to determine that company policies and procedures were communicated to personnel via the security and compliance application.	No exceptions noted.
CC2.2.2	AllVoices management maintains a security and privacy e-mail inbox and communicates to internal users via company policy that security and privacy concerns may be reported via this e-mail inbox for management to evaluate.	Inspected the security and privacy e-mail inbox and the Incident Response Policy to determine that management maintained a security and privacy e-mail inbox and communicated internally via the policy that personnel may submit security and privacy concerns via the e-mail address.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC2.2.3	The Incident Response Plan outlines the processes for identifying, prioritizing, communicating, assigning, and tracking incidents through resolution and is communicated to personnel via the security and compliance application.	Inspected the Incident Response Plan within the security and compliance application to determine that the policy and procedure outlined the processes for identifying, prioritizing, communicating, assigning, and tracking incidents through resolution and was communicated to personnel via the security and compliance application.	No exceptions noted.
CC2.2.4	AllVoices has established a Code of Conduct outlining ethical expectations, behavioral standards, and ramifications for noncompliance. The Code of Conduct is communicated to personnel via the security and compliance application.	Inspected the Code of Conduct within the security and compliance application to determine that AllVoices established a Code of Conduct which outlined the ethical expectations, behavioral standards, and ramifications for noncompliance and that the document was communicated to personnel via the security and compliance application.	No exceptions noted.
CC2.2.5	Senior management meets with the board of directors quarterly to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	Inspected the board of directors meeting minutes for a sample of quarters during the review period and determined that senior management met with the board of directors quarterly during the review period to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	No exceptions noted.
CC2.2.6	Personnel complete an information security training program within 60 days of hire and on an annual basis thereafter to help them understand their obligations and responsibilities related to security.	Inspected the security awareness training records for a sample of employees hired during the review period to determine that each employee sampled completed an information security training program within 60 days of hire.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
		Inspected the security awareness training records for a sample of employees with tenure greater than a year to determine that each employee sampled had completed a security awareness training program within the 12 months preceding the end of the review period.	No exceptions noted.
CC2.2.7	Personnel are required to acknowledge the Code of Conduct and the company information security policies within 30 days of hire.	Inspected the policy and procedure acknowledgement records for a sample of employees hired during the review period to determine that each employee sampled acknowledged the Code of Conduct and the company information security policies within 30 days of hire.	No exceptions noted.
CC2.2.8	Personnel responsible for the design, implementation, and management of the organization’s policies and procedures are documented as owners within the policies and procedures. Policy owners are required to review and approve their owned policies and procedures on at least an annual basis.	Inspected a sample of the company policies and procedures to determine that personnel responsible for the design, implementation, and management of the policies and procedures were documented as owners within each policy and procedure sampled and that the owners reviewed the sampled policies and procedures within the 12 months preceding the end of the review period.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	AllVoices security commitments are communicated externally on its public facing website through product description pages and its privacy notice.	Inspected the externally facing website to determine that AllVoices security commitments were communicated via the website through product descriptions and its privacy notice.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC2.3.2	AllVoices management maintains a security and privacy e-mail inbox and communicates to external users via the public website that security and privacy concerns may be reported via this e-mail address for management to evaluate.	Inspected the security and privacy e-mail inbox and public company website to determine that management maintained a security and privacy e-mail inbox and communicated externally via the website that users may submit security and privacy concerns via the e-mail address for management to evaluate.	No exceptions noted.
CC3.0: Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Company policies are prefaced by the organization's objective the policy is intended to achieve. Policies are communicated to personnel via the security and compliance application.	Inspected a sample of company policies and procedures to determine that each policy sampled was prefaced by an organizational objective which the policy was intended to achieve.	No exceptions noted.
		Inspected the policy and procedure module within the security and compliance platform to determine that company policies and procedures were communicated to personnel via the security and compliance application.	No exceptions noted.
CC3.1.2	Formal risk management policies and procedures are in place which define the company risk assessment and mitigation procedures. The policies and procedures are reviewed and approved by the CEO on at least an annual basis.	Inspected the Risk Management Policy to determine that formal risk management policies and procedures were in place which defined the company risk assessment and mitigation procedures and to determine that the CEO reviewed and approved the policy within the 12 months preceding the end of the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Formal risk management policies and procedures are in place which define the company risk assessment and mitigation procedures. The policies and procedures are reviewed and approved by the CEO on at least an annual basis.	Inspected the Risk Management Policy to determine that formal risk management policies and procedures were in place which defined the company risk assessment and mitigation procedures and to determine that the CEO reviewed and approved the policy within the 12 months preceding the end of the review period.	No exceptions noted.
CC3.2.2	AllVoices identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets.	Inspected the asset inventory to determine that AllVoices identified its information assets and maintained an inventory of its system components, owners, and their support of its information assets.	No exceptions noted.
CC3.2.3	A formal risk assessment, which includes the identification of relevant internal and external threats, fraud risks, and an analysis of risks associated with the identified threats is performed on an annual basis.	Inspected the completed annual risk assessment to determined that a risk assessment which included the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats was performed within the 12 months preceding the end of the review period.	No exceptions noted.
CC3.2.4	Vendor management policies and procedures are implemented and define a framework for the management of risks associated with vendors.	Inspected the Third-Party Management Policy to determine that vendor management policies and procedures were implemented and defined a framework for the management of risks associated with vendors.	No exceptions noted.
CC3.2.5	A vendor repository is maintained that includes a risk classification associated with each of the company's vendors.	Inspected the vendor repository to determine that a vendor repository was maintained and included risk classifications associated with each of the company's vendors.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC3.2.6	Management obtains and reviews a third-party assurance report of its subservice organizations on an annual basis.	Inspected the most recently obtained and reviewed third-party assurance report for the subservice organization specified by the company to determine that management obtained and reviewed the third-party assurance report for the subservice organization during the review period.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Risk management policies and procedures are in place which require an assessment of fraud risks as a component of the risk assessment process.	Inspected the Risk Management Policy to determine that the policy required an assessment of fraud risks as a component of the risk assessment process.	No exceptions noted.
CC3.3.2	A formal risk assessment, which includes the identification of relevant internal and external threats, fraud risks, and an analysis of risks associated with the identified threats is performed on an annual basis.	Inspected the completed annual risk assessment to determined that a risk assessment which included the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats was performed within the 12 months preceding the end of the review period.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A formal risk assessment, which includes the identification of relevant internal and external threats, fraud risks, and an analysis of risks associated with the identified threats is performed on an annual basis.	Inspected the completed annual risk assessment to determined that a risk assessment which included the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats was performed within the 12 months preceding the end of the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC4.0: Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes needed are tracked to remediation.	Inspected the completed user access review for a sample of quarters during the review period to determine that system owners conducted a user access review of production servers, databases and applications to validate internal user access was commensurate with job responsibilities and that identified access changes needed were tracked through resolution for each quarter sampled.	No exceptions noted.
CC4.1.2	AllVoices uses a security and compliance monitoring application to perform a continuous assessment over defined internal controls and to alert management of identified deficiencies.	Inspected the security and compliance monitoring application to determine that the application performed continuous assessments over defined internal controls and alerted management of identified deficiencies.	No exceptions noted.
CC4.1.3	Vulnerability scans are executed weekly on production systems. Identified vulnerabilities are tracked through the security and compliance platform in accordance with predefined SLAs.	Inquired of the VP of engineering regarding vulnerability scans to determine that vulnerability scans were executed on a weekly basis and identified vulnerabilities were tracked through the security and compliance platform.	No exceptions noted.
		Inspected the vulnerability scanning application configurations and tracking dashboards within the security and compliance monitoring tool to determine that vulnerability scans were executed weekly on production systems and that identified vulnerabilities were tracked through the security and compliance platform in accordance with predefined SLAs.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC4.1.4	A third party is engaged to conduct a network and application penetration test of the production environment at least annually. Results are reviewed and high priority findings are tracked through resolution.	Inspected the most recent penetration test report to determine that a third part was engaged to perform an application penetration test during the 12 months preceding the end of the review period.	No exceptions noted.
		Inspected the penetration re-test report to determine that high priority findings were tracked through resolution.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes needed are tracked to remediation.	Inspected the completed user access review for a sample of quarters during the review period to determine that system owners conducted a user access review of production servers, databases and applications to validate internal user access was commensurate with job responsibilities and that identified access changes needed were tracked through resolution for each quarter sampled.	No exceptions noted.
CC4.2.2	Senior management meets with the board of directors quarterly to review business objectives, company initiatives, resource needs, and risk management activities, including results from external assessments.	Inspected the board of directors meeting minutes for a sample of quarters during the review period to determine that senior management met with the board of directors for each quarter during the review period sampled to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	No exceptions noted.
CC4.2.3	AllVoices uses a security and compliance monitoring application to perform a continuous assessment over defined internal controls and to alert management of identified deficiencies.	Inspected the security and compliance monitoring application to determine that the application performed continuous assessments over defined internal controls and alerted management of identified deficiencies.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC5.0: Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	AllVoices identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets.	Inspected the asset inventory to determine that AllVoices identified its information assets and maintained an inventory of its system components, owners, and their support of its information assets.	No exceptions noted.
CC5.1.2	A risk register is maintained which records identified risks and proposed or implemented tasks to mitigate identified risks.	Inspected the risk register to determine that a risk register was maintained which recorded identified risks and proposed or implemented tasks to mitigate identified risks during the review period.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	AllVoices identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets.	Inspected the asset inventory to determine that AllVoices identified its information assets and maintained an inventory of its system components, owners, and their support of its information assets.	No exceptions noted.
CC5.2.2	A risk register is maintained which records identified risks and proposed or implemented tasks to mitigate identified risks.	Inspected the risk register during the review period to determine that a risk register was maintained which recorded identified risks and proposed or implemented tasks to mitigate identified risks.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Company policies and procedures are documented and communicated to personnel via the security and compliance application.	Inspected the policy and procedure module within the security and compliance platform to determine that company policies and procedures were communicated to personnel via the security and compliance application.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC5.3.2	Personnel are required to acknowledge the Code of Conduct and the company information security policies within 30 days of hire.	Inspected the policy and procedure acknowledgement records for a sample of employees hired during the review period to determine that each employee sampled acknowledged the Code of Conduct and the company information security policies within 30 days of hire.	No exceptions noted.
CC5.3.3	Personnel responsible for the design, implementation, and management of the organization’s policies and procedures are documented as owners within the policies and procedures. Policy owners are required to review and approve their owned policies and procedures on at least an annual basis.	Inspected a sample of the company policies and procedures to determine that personnel responsible for the design, implementation, and management of the policies and procedures were documented as owners within each policy and procedure sampled and that the owners reviewed the sampled policies and procedures within the 12 months preceding the end of the review period.	No exceptions noted.
CC6.0: Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	AllVoices identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets.	Inspected the asset inventory to determine that AllVoices identified its information assets and maintained an inventory of its system components, owners, and their support of its information assets.	No exceptions noted.
CC6.1.2	Access control policies and procedures are in place to guide personnel in the requirements for authorizing, adding, modifying, and removing user access privileges to company systems.	Inspected the Access Control Policy to determine that access control policies and procedures were in place to guide personnel in the requirements for authorizing, adding, modifying, and removing user access privileges to company systems.	No exceptions noted.
CC6.1.3	Users are assigned unique IDs to access production resources and supporting applications.	Inspected the user access listings to the company cloud account, network directory, and development version control system to determine that users were assigned unique IDs to access production	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC6.1.4	Internal access to systems and applications with service data requires multi-factor authentication.	Inspected user authentication configurations for a sample of user with access to access to systems and applications with service data to determine that internal access to systems and applications with service data required multi-factor authentication for each sampled user.	No exceptions noted.
CC6.1.5	Formal policies for password strength and use of authentication mechanisms are in place and include requirements for the following: • Minimum length of eight characters • At least one uppercase • At least one lowercase • At least one number	Inspected the Access Control policy to determine that the policy defined requirements for password strength and use of authentication mechanisms and that the policy required passwords to contain: • Minimum length of eight characters • At least one uppercase • At least one lowercase • At least one number	No exceptions noted.
		Inspected the password configurations for the cloud infrastructure provider to determine that password policies were configured in compliance with the password policy.	No exceptions noted.
CC6.1.6	Administrative access to production servers and databases is restricted to authorized members of the engineering team via predetermined group access privileges.	Inquired of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access permissions.	No exceptions noted.
		Inspected the user account listings of the administrative user groups within the cloud console with the assistance of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access privileges.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.1.7	Internal users are provisioned access to systems based on role as defined in the access matrix upon formal notification from HR of the employee role and start date.	Inspected the HR employment notifications for a sample of employees hired during the review period to determine that HR notified engineering of employment start date and role for each employee sampled.	No exceptions noted.
		Inspected the access matrix and user access privileges for a sample of employees hired during the review period to determine that engineering personnel provisioned access to systems based on roles as defined in the access matrix.	No exceptions noted.
CC6.1.8	Service data is encrypted at rest.	Inspected the production database encryption configurations to determine that service data was encrypted at rest.	No exceptions noted.
CC6.1.9	Customers authenticate to the production application via username and password. Passwords must meet the following minimum standards: • Minimum length of eight characters • Character complexity • Lockout after five invalid attempts	Inspected the hard coded production application password requirements to determine that customer authentication to the application required a unique username and password which was required to meet the following minimum standards: • Minimum length of eight characters • Character complexity • Lockout after five invalid attempts	No exceptions noted.
CC6.1.10	Network security groups are configured to restrict inbound traffic from external sources to TCP traffic via port 443.	Inspected the port configurations for a sample of network security group rule sets to determine that firewall configurations restricted inbound traffic from external sources to TCP traffic via port 443 for each network security group during the review period sampled.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.1.11	A WAF is in place and configured to restrict inbound transmissions from the Internet to authorized sources.	Inspected the WAF dashboards and rule set configurations to determine that a WAF was in place and configured to restrict inbound transmissions from the Internet to authorized sources.	No exceptions noted.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Internal users are provisioned access to systems based on role as defined in the access matrix upon formal notification from HR of the employee role and start date.	Inspected the HR employment notifications for a sample of employees hired during the review period to determine that HR notified engineering of employment start date and role for each employee sampled.	No exceptions noted.
		Inspected the access matrix and user access privileges for a sample of employees hired during the review period to determine that engineering personnel provisioned access to systems based on roles as defined in the access matrix.	No exceptions noted.
CC6.2.2	Upon employee termination, infrastructure and application access is removed within one business day.	Inspected the employee user account access status within the company infrastructure and supporting applications for a sample of employees terminated during the review period to determine that infrastructure and application access was removed within one business day for each employee sampled.	No exceptions noted.
CC6.2.3	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes needed are tracked to remediation.	Inspected the completed user access review for a sample of quarters during the review period to determine that system owners conducted a user access review of production servers, databases and applications to validate internal user access was commensurate with job responsibilities and that identified access changes needed were tracked through resolution for each quarter sampled.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.			
CC6.3.1	Administrative access to production servers and databases is restricted to authorized members of the engineering team via predetermined group access privileges.	Inquired of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access permissions.	No exceptions noted.
		Inspected the user account listings of the administrative user groups within the cloud console with the assistance of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access privileges.	No exceptions noted.
CC6.3.2	Internal users are provisioned access to systems based on role as defined in the access matrix upon formal notification from HR of the employee role and start date.	Inspected the HR employment notifications for a sample of employees hired during the review period to determine that HR notified engineering of employment start date and role for each employee sampled.	No exceptions noted.
		Inspected the access matrix and user access privileges for a sample of employees hired during the review period to determine that engineering personnel provisioned access to systems based on roles as defined in the access matrix.	No exceptions noted.
CC6.3.3	Upon employee termination, infrastructure and application access is removed within one business day.	Inspected the employee user account access status within the company infrastructure and supporting applications for a sample of employees terminated during the review period to determine that infrastructure and application access was removed within one business day for each employee sampled.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.3.4	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes needed are tracked to remediation.	Inspected the completed user access review for a sample of quarters during the review period to determine that system owners conducted a user access review of production servers, databases and applications to validate internal user access was commensurate with job responsibilities and that identified access changes needed were tracked through resolution for each quarter sampled.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.			
	AWS is responsible for ensuring access to its facilities and the physical information assets hosted within its facilities is restricted to authorized personnel.		
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.			
	AWS is responsible for ensuring physical media containing production data is securely sanitized or destroyed prior to being removed from its data center or protected areas within its data center facilities.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Encryption is used to protect the transmission of data over the Internet.	Inspected the production application encryption configurations to determine that encryption was used to protect the transmission of data over the internet.	No exceptions noted.
CC6.6.2	Firewall configurations restrict inbound traffic from external sources to TCP traffic via port 443.	Inspected the port configurations for a sample of network security group rule sets to determine that firewall configurations restricted inbound traffic from external sources to TCP traffic via port 443 for each network security group during the review period sampled.	No exceptions noted.
CC6.6.3	A WAF is in place and configured to restrict inbound transmissions from the Internet to authorized sources.	Inspected the WAF dashboards and rule set configurations to determine that a WAF was in place and configured to restrict inbound transmissions from the Internet to authorized sources.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.6.4	Internal access to systems and applications with service data requires multi-factor authentication.	Inspected user authentication configurations for a sample of user with access to access to systems and applications with service data to determine that internal access to systems and applications with service data required multi-factor authentication for each sampled user.	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.			
CC6.7.1	Encryption is used to protect the transmission of data over the Internet.	Inspected the production application encryption configurations to determine that encryption was used to protect the transmission of data over the internet.	No exceptions noted.
CC6.7.2	Administrative access to production servers and databases is restricted to authorized members of the engineering team via predetermined group access privileges.	Inquired of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access permissions.	No exceptions noted.
		Inspected the user account listings of the administrative user groups within the cloud console with the assistance of the VP of engineering to determine that administrative access to production servers and databases was restricted to authorized members of the engineering team via predetermined group access privileges.	No exceptions noted.
CC6.7.3	Company laptops are configured with full disk encryption.	Inspected the laptop disk encryption configurations for a sample of current employees to determine that company laptops were configured with full disk encryption for the laptop of each employee sampled.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.			
CC6.8.1	Standard infrastructure base images are used to enforce configurations for production resources.	Inspected the base images for production resources to determine that standard infrastructure base images were used to enforce configurations for production resources.	No exceptions noted.
CC6.8.2	Malware detection software is installed on the laptops of employees with access to production infrastructure.	Inspected the malware detection software configured on employee workstations for a sample of employees with access to production infrastructure during the review period to determine that malware detection software was installed on the laptops of each employee sampled.	No exceptions noted.
CC7.0: System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Documented event and incident management policies and procedures are in place which outline the processes and responsibilities for the detection and monitoring for vulnerabilities.	Inspected the Incident Response Plan to determine that documented event and incident management policies and procedures were in place which outlined the processes and responsibilities for the detection and monitoring of vulnerabilities.	No exceptions noted.
CC7.1.2	Standard infrastructure base images are used to enforce configurations for production resources.	Inspected the base images for production resources to determine that standard infrastructure base images were used to enforce configurations for production resources.	No exceptions noted.
CC7.1.3	Malware detection software is installed on the laptops of employees with access to production infrastructure.	Inspected the malware detection software configured on employee workstations for a sample of employees with access to production infrastructure during the review period to determine that malware detection software was installed on the laptops of each employee sampled.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC7.1.4	Vulnerability scans are executed weekly on production systems. Identified vulnerabilities are tracked through the security and compliance platform in accordance with predefined SLAs.	Inquired of the VP of engineering regarding vulnerability scans to determine that vulnerability scans were executed on a weekly basis and identified vulnerabilities were tracked through the security and compliance platform.	No exceptions noted.
		Inspected the vulnerability scanning application configurations and tracking dashboards within the security and compliance monitoring tool to determine that vulnerability scans were executed weekly on production systems and that identified vulnerabilities were tracked through the security and compliance platform in accordance with predefined SLAs.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Management has implemented intrusion detection tools to monitor production traffic for potential security events.	Inspected the intrusion detection tool dashboards and example detection alerts during the review period to determine that management had implemented an intrusion detection tool to monitor production traffic for potential security events.	No exceptions noted.
CC7.2.2	Logging and monitoring software is used to collect data from servers and endpoints.	Inspected the cloud infrastructure logging configurations to determine that logging and monitoring software was used to collect data from servers and endpoints.	No exceptions noted.
CC7.2.3	Alerting software is used to notify impacted teams of potential security events. Engineering personnel track identified events through resolution.	Inspected the security and compliance monitoring application to determine alerting software was used to notify impacted teams of potential security events.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
		Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that engineering personnel tracked identified events through resolution for each sample selected.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	Inspected the Incident Response Plan to determine that the policy and procedure outlined the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	No exceptions noted.
CC7.3.2	AllVoices management maintains a security and privacy e-mail inbox and communicates to internal users via company policy that security and privacy concerns may be reported via this e-mail inbox for management to evaluate.	Inspected the security and privacy e-mail inbox and the Incident Response Policy to determine that management maintained a security and privacy e-mail inbox and communicated internally via the policy that personnel may submit security and privacy concerns via the e-mail address.	No exceptions noted.
CC7.3.3	Designated incident response personnel track identified events and incidents in accordance with the Incident Response Plan.	Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that designated incident response personnel tracked identified events and incidents in accordance with the Incident Response Plan for each sample selected.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	Inspected the Incident Response Plan to determine that the policy and procedure outlined the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC7.4.2	Designated incident response personnel track identified events and incidents in accordance with the Incident Response Plan.	Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that designated incident response personnel tracked identified events and incidents in accordance with the Incident Response Plan for each sample selected.	No exceptions noted.
CC7.4.3	A lessons learned exercise is documented within incident investigation reports after each reported incident.	Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that a lessons learned exercise was documented for each reported incident sampled.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	Inspected the Incident Response Plan to determine that the policy and procedure outlined the process of identifying, prioritizing, communicating, assigning, and tracking events and incidents through resolution.	No exceptions noted.
CC7.5.2	Designated incident response personnel track identified events and incidents in accordance with the Incident Response Plan.	Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that designated incident response personnel tracked identified events and incidents in accordance with the Incident Response Plan for each sample selected.	No exceptions noted.
CC7.5.3	A lessons learned exercise is documented within incident investigation reports after each reported incident.	Inspected the incident tracking ticketing system and incident investigation report for a sample of incidents during the review period to determine that a lessons learned exercise was documented for each reported incident sampled.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC8.0: Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change management policies and procedures are in place that govern the system development life cycle, including the tracking, testing, and approving changes.	Inspected the Operations Security Policy and the Secure Development Policy to determine that change management policies and procedures were in place to govern the system development life cycle, including the tracking, testing, and approving of changes.	No exceptions noted.
CC8.1.2	Standard infrastructure base images are used to enforce configurations for production resources.	Inspected the base images for production resources to determine that standard infrastructure base images were used to enforce configurations for production resources.	No exceptions noted.
CC8.1.3	Production application changes are tested via automated test scripts prior to deployment into production.	Inquired of the VP of engineering to determine the development repositories supporting the production application and that changes were tested via automated test scripts prior to deployment into production.	No exceptions noted.
		Inspected the automated testing completion records within the change tickets for a sample of production application changes during the review period to determine that production application changes were tested via automated test scripts prior to deployment to production for each change sampled.	No exceptions noted.
CC8.1.4	An independent engineer peer reviews and approves code merge requests before the code change is committed into the master branch.	Inspected the change tickets for a sample of code merges during the review period to determine that an independent engineer peer reviewed and approved each code merge request sampled prior to the change being committed into the master branch.	No exceptions noted.

Control #	Description of Service Organization’s Controls	Service Auditor’s Tests of Controls	Test Results
CC8.1.5	System users who make changes to the development system are unable to deploy their changes to production without independent approval.	Inspected the branch rule configurations and determined that system users who make changes to the development system were unable to deploy their changes to production without independent approval.	No exceptions noted.
CC8.1.6	The production environment is segregated from the development and staging environments.	Inspected the company VPCs, Kubernetes clusters, and databases within the cloud infrastructure to determine that the production environment was segregated from the development and staging environments.	No exceptions noted.
CC8.1.8	Production data is not used in the development or staging environments.	Inquired of the VP of engineering to determine that production data was not used in the development or staging environments.	No exceptions noted.
		Inspected exports from the staging and development databases to determine that production data was not used in the development or staging environments.	No exceptions noted.
CC9.0: Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Management maintains an insurance policy to transfer the financial risk associated with a cybersecurity incident.	Inspected the cyber insurance policy to determine that management maintained an insurance policy to transfer the financial risk associated with a cybersecurity incident.	No exceptions noted.
CC9.1.2	A risk register is maintained which records identified risks and proposed or implemented tasks to mitigate identified risks.	Inspected the risk register to determine that a risk register was maintained which recorded identified risks and proposed or implemented tasks to mitigate identified risks during the review period.	No exceptions noted.

Control #	Description of Service Organization's Controls	Service Auditor's Tests of Controls	Test Results
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Vendor management policies and procedures are implemented and define a framework for the management of risks associated with vendors.	Inspected the Third-Party Management Policy to determine that vendor management policies and procedures were implemented and defined a framework for the management of risks associated with vendors.	No exceptions noted.
CC9.2.2	A vendor repository is maintained that includes a risk classification associated with each of the company's vendors.	Inspected the vendor repository to determine that a vendor repository was maintained and included risk classifications associated with each of the company's vendors.	No exceptions noted.
CC9.2.3	Management obtains and reviews a third-party assurance report of its subservice organizations on an annual basis.	Inspected the most recently obtained and reviewed third-party assurance report for the subservice organization specified by the company to determine that management obtained and reviewed the third-party assurance report for the subservice organization during the review period.	No exceptions noted.