COALFIRE
CONTROLS

# Report on Nuance Communications, Inc.'s Description of Its Dragon Medical One and Dragon Medical SpeechKit and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period May 1, 2024 to April 30, 2025

SOC 2® - SOC for Service Organizations: Trust Services Criteria

NUANCE®

# Table of Contents

## Section 1

## Section 2

## Section 3

## Section 4

# Section 1

# Independent Service Auditor’s Report

# Independent Service Auditor's Report

To: Nuance Communications, Inc. ("Nuance")

## Scope

We have examined Nuance's accompanying description found in Section 3 titled "Nuance Communications, Inc.'s Description of Its Dragon Medical One and Dragon Medical SpeechKit Throughout the Period May 1, 2024 to April 30, 2025" (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 (With Revised Implementation Guidance—2022*), in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Nuance's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Nuance uses a subservice organization to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nuance, to achieve Nuance's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuance's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nuance's 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.

Nuance uses Microsoft Azure to provide a wide variety of services including HR functions and vendor management services. The description indicates that complementary corporate-level controls of Microsoft Azure that are suitably designed and operating effectively are necessary, along with controls at Nuance, to achieve Nuance's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuance's controls, the applicable trust services criteria, and the types of complementary corporate-level controls assumed in the design of Nuance's controls. The description does not disclose the actual controls at Microsoft Azure. Our examination did not include the services provided by Microsoft Azure, and we have not evaluated the suitability of the design or operating effectiveness of such complementary corporate-level controls.

## Service Organization's Responsibilities

Nuance 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 Nuance's service commitments and system requirements were achieved. In Section 2, Nuance has provided the accompanying assertion titled "Assertion of Nuance Communications, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Nuance 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.

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

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

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

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

### Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. 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 or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

## Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories" of this report.

## Opinion

In our opinion, in all material respects—

a. The description presents Nuance's Dragon Medical One and Dragon Medical SpeechKit that were designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Nuance's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if Microsoft Azure and the subservice organization applied the complementary controls assumed in the design of Nuance's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Nuance's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary corporate-level controls and complementary subservice organization controls assumed in the design of Nuance's 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 Nuance, user entities of Nuance's Dragon Medical One and Dragon Medical SpeechKit during some or all of the period May 1, 2024 to April 30, 2025, business partners of Nuance subject to risks arising from interactions with the Dragon Medical One and Dragon Medical SpeechKit, 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, the subservice organization, and other parties.
- Internal control and its limitations.
- Complementary corporate-level controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report should only be used in conjunction with the service organization controls report covering the description of Microsoft Azure addressing corporate functions. This report is not intended to be, and should not be, used by anyone other than these specified parties.

If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, 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 Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Greenwood Village, Colorado
June 27, 2025

# Section 2

# Assertion of Nuance Communications, Inc. Management

NUANCE

Partner Security Engineering Manager
Nuance Communications (a Microsoft company)
15 Wayside Road
Burlington, MA 01803

### Assertion of Nuance Communications, Inc. ("Nuance") Management

We have prepared the accompanying description titled "Nuance Communications, Inc.'s Description of Its Dragon Medical One and Dragon Medical SpeechKit Throughout the Period May 1, 2024 to April 30, 2025" (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 (With Revised Implementation Guidance—2022*), in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Dragon Medical One and Dragon Medical SpeechKit that may be useful when assessing the risks arising from interactions with Nuance's system, particularly information about system controls that Nuance has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

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

Nuance uses Microsoft Azure for a wide variety of services including HR functions and vendor management services. The description indicates that complementary corporate-level controls of Microsoft Azure that are suitably designed and operating effectively are necessary, along with controls at Nuance, to achieve Nuance's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuance's controls, the applicable trust services criteria, and the types of complementary corporate-level controls assumed in the design of Nuance's controls. The description does not disclose the actual controls at Microsoft Azure.

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

a. The description presents Nuance's Dragon Medical One and Dragon Medical SpeechKit that were designed and implemented throughout the period May 1, 2024 to April 30, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Nuance's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if Microsoft Azure and the subservice organization applied the complementary controls assumed in the design of Nuance's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2024 to April 30, 2025, to provide reasonable assurance that Nuance's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary corporate-level controls and complementary subservice organization controls assumed in the design of Nuance's controls operated effectively throughout that period.

Nuance Communications, Inc.

# Section 3

# Nuance Communications, Inc.’s Description of Its Dragon Medical One and Dragon Medical SpeechKit Throughout the Period May 1, 2024 to April 30, 2025

# Type of Services Provided

Nuance Communications, Inc., a Microsoft company, is a provider of voice and language solutions for businesses and consumers around the world. Nuance Healthcare creates clinical understanding solutions that drive smart, efficient decisions across healthcare. Numerous Physicians and healthcare facilities worldwide leverage Nuance Healthcare's voice-enabled clinical documentation and analytics solutions to support the physician in any clinical workflow and on any device.

## Dragon Medical One and Dragon Medical SpeechKit

Dragon Medical One and Dragon Medical SpeechKit are a secure, cloud-based speech recognition solution that allows clinicians to document the complete patient story using voice while allowing healthcare organizations to easily deploy medical speech recognition across their enterprise.

Highly scalable and ready-to-use, Dragon Medical One and Dragon Medical SpeechKit provide cloud-based clinical speech recognition across an existing infrastructure of Windows-based devices, including virtualized and remote-access PCs. The lightweight Windows client application downloads and installs in minutes and provides a secure connection to the Nuance cloud. It delivers cross-channel access to user voice profiles, real-time speech-to-text and the latest medical dictionary, terms, phrases, and clinical formatting rules to ensure a fast and accurate speech recognition experience. Additional features include specialty-specific medical language models, automated user accent detection and gain control, custom vocabularies and templates, and voice-based correction.

Dragon Medical One and Dragon Medical SpeechKit can be installed on any clinical workstation or laptop in just minutes without the need for complex configurations. Once installed, clinicians simply open the application from the Windows Start menu, place the cursor where they want speech-recognized text to appear, and start dictating into any clinical, or non-clinical, Windows-based application (e.g., EHR, Microsoft Outlook, and Microsoft Word). Standard preferred dictation hardware, such as the PowerMic III, is plug-and-play, but other hardware is also supported. Zero voice profile training, automatic accent detection, and profiles that continue to adapt and improve over time, ensure an optimal clinician experience from the start.

Dragon Medical SpeechKit - is a series of SDKs provided by Nuance to add cloud-based, real-time speech recognition to your desktop or mobile app.

The system description in this section of the report details the Dragon Medical One and the Dragon Medical SpeechKit. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

# Dragon Medical One and Dragon Medical SpeechKit Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Dragon Medical One and Dragon Medical SpeechKit. Commitments are communicated within Master Hosted Service Agreements and Hosted Services Orders.

System requirements are specifications regarding how Dragon Medical One and Dragon Medical SpeechKit should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to Dragon Medical One and Dragon Medical SpeechKit include the following:

| Trust Services Category | Service Commitments | System Requirements |
|---|---|---|
| **Security** | • Nuance will provide 24/7 monitoring and maintenance 365 days a year through the Service Reliability Center (SRC).<br>• Nuance will perform platform maintenance (scheduled and emergency) and upgrades via SRC personnel.<br>• Nuance will provide incident management support and track incidents in a web-based ticket tracking system.<br>• Nuance will notify a specific customer of any incident that affects their data.<br>• Nuance will notify customers of any known events based on the applicable severity level. | • Logical access standards<br>• Physical access standards<br>• Employee provisioning and deprovisioning standards<br>• Access reviews<br>• Encryption standards<br>• Intrusion detection and prevention standards<br>• Risk and vulnerability management standards<br>• Configuration management<br>• Incident handling standards<br>• Change management standards<br>• Vendor management |
| **Availability** | • Nuance will use commercially reasonable efforts to maintain operational system uptime.<br>• Nuance will provide redundancy for network components and servers to ensure the high availability of the hosted services.<br>• Nuance will maintain application and infrastructure hosting in at least two geographically redundant data center locations spanning multiple power grids.<br>• Nuance will use commercially reasonable efforts to manage capacity requirements based on customer capacity forecasts provided to Nuance.<br>• Nuance will perform maintenance to keep the hosted services' infrastructure in optimal working order. | • System monitoring<br>• Backup and recovery standards<br>• Physical and environmental protections |
| **Confidentiality** | • Nuance will only permit the disclosure of confidential information if such disclosure is in response to an order of a court or other governmental body or otherwise required by law.<br>• Nuance will not use confidential information for purposes other than in the regular course of providing services.<br>• Nuance will return or destroy all confidential information in tangible form upon written request or upon the expiration or termination of the service.<br>• Nuance will use the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, disclosure, or publication of confidential information to third parties as it uses to protect its own confidential information. | • Data classification<br>• Retention and destruction standards<br>• Data handling standards<br>• Internal confidentiality standards<br>• Information sharing standards |

# The Components of the System Used to Provide the Services

The boundaries of Dragon Medical One and Dragon Medical SpeechKit are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Dragon Medical One and Dragon Medical SpeechKit.

The components that directly support the services provided to customers are described in the subsections below.

## Infrastructure

Nuance utilizes Microsoft Azure to provide the resources to host Dragon Medical One and Dragon Medical SpeechKit. Nuance leverages the experience and resources of Microsoft Azure to scale quickly and securely as necessary to meet current and future demand. However, Nuance is responsible for designing and configuring the Dragon Medical One and Dragon Medical SpeechKit architecture within Microsoft Azure to ensure the availability, security, and resiliency requirements are met.

Dragon Medical One and Dragon Medical SpeechKit are supported by active instances at three Microsoft Azure cloud computing data centers providing highly scalable, responsive, and available environments. Customer transactions are dispatched to one of five data centers, West US, North Central US, East US, Berlin Germany, or Frankfurt Germany by Azure traffic management, and traffic loads are balanced across components within each center.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

| Data Hosting | |
|---|---|
| **Provider** | **Business Function** |
| Microsoft Azure | Data center facility |

| Infrastructure | | | |
|---|---|---|---|
| **Production Tool** | **Business Function** | **Operating System** | **Hosted Location** |
| Microsoft Azure Management Console | Allows system administrators to manage and maintain in-scope servers, DBs, and services. | Linux RHEL<br>Windows OS | Microsoft Azure Cloud PaaS |
| Production servers | Linux and Windows servers supporting the in-scope systems. | Linux RHEL<br>Windows OS | Microsoft Azure Cloud PaaS |
| Azure SQL | DBs supporting the logic of the in-scope systems. | Linux RHEL<br>Windows OS | Microsoft Azure Cloud PaaS |
| Virtual private network (VPN) | Provides remote access to the in-scope systems with multifactor authentication. | Linux RHEL<br>Windows OS | Microsoft Azure Cloud PaaS |

## Software

Software consists of the programs and software that support Dragon Medical One and Dragon Medical SpeechKit (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Dragon Medical One and Dragon Medical SpeechKit include the following applications, as shown in the table below:

| Software | |
|---|---|
| **Production Application** | **Business Function** |
| Prometheus, Grafana, and Azure Monitor | System monitoring |
| Nuance Management Server | Backup and replication |
| Microsoft Sentinel | Security information and event management (SIEM), logging system |
| Azure Monitor and Prometheus | Infrastructure monitoring |
| WSUS & RHEL Repos | Patch management |
| WSUS & RHEL Repos | File integrity monitoring |
| MDE / Windows Defender | Antivirus |
| MDE / Windows Defender | Intrusion detection and prevention |
| ServiceNow | Ticketing system |
| Ansible | Configuration management |
| Kafka and DataBricks | Logging |

## People

Nuance develops, manages, and secures Dragon Medical One and Dragon Medical SpeechKit via separate departments. The responsibilities of these departments are defined in the following table:

| People | |
|---|---|
| **Group/Role Name** | **Function** |
| Executive Management | Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives. |
| Engineering | Responsible for the development, testing, deployment, and maintenance of new code for Dragon Medical One and Dragon Medical SpeechKit. |
| Information Security (InfoSec) | Responsible for managing access controls and the security of the production environment. |
| Product Management | Responsible for overseeing the product life cycle, including adding new product functionality. |
| Human Resources (HR) | Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process. |

| People | |
|---|---|
| Group/Role Name | Function |
| Technical Support Team | Responsible for working directly with customers. |
| Site Reliability Engineering (SRE) | Responsible for monitoring of the systems. |

## Procedures

Procedures include the automated and manual procedures involved in the operation of Dragon Medical One and Dragon Medical SpeechKit. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Dragon Medical One and Dragon Medical SpeechKit:

| Procedures | |
|---|---|
| Procedure | Description |
| Logical Access | How the Company restricts logical access, provides and removes that access, and prevents unauthorized access. |
| System Operations | How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations. |
| Change Management | How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made. |
| Risk Mitigation | How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners. |

## Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Dragon Medical One and Dragon Medical SpeechKit production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

The following table details the types of data contained in the production application for Dragon Medical One and Dragon Medical SpeechKit:

| Data | | |
|---|---|---|
| **Production Application** | **Description** | **Data Store** |
| Customer Information | Refers to user account, licensing and configuration information. | NMS MS SQL Server Database |
| Speech Profiles | Refers to personalized settings that enhance the accuracy and efficiency of speech recognition systems. These personalized settings include language and acoustical statistics of how an individual user pronounces sounds and uses words in a given language. These profiles are tailored to individual users, taking into account their unique voice characteristics, accents, and speaking styles. | Azure File System |
| Persisted audio and text files, including PHI | Refers to audio recordings and text transcripts that are persistently stored and could contain Protected Health Information (PHI), such as patient identifiers, medical histories, or treatment details. These files are retained specifically for the purpose of training and refining speech recognition profiles, ensuring improved accuracy and personalization while adhering to strict privacy and security standards. | Azure File System |
| Server Images | Refers to virtual machine snapshots or disk images that capture the full state of a server, including its operating system, configurations, and stored data. | Azure Backup Services |
| Server configuration information | Refers to the stored details that define how a server is set up and operates, including system settings, network configurations, installed software, and security policies. | Azure DevOps managed repositories and Ansible Platform |
| Code Base | Refers to the complete set of software assets used in a system, including vendor-provided software and firmware, associated licenses, and internally developed application product code. | Azure DevOps managed repositories |

# System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from May 1, 2024 to April 30, 2025.

# The Applicable Trust Services Criteria and Related Controls

## Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality:* Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability and confidentiality a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Information and communication:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

# Control Environment

## Organizational Structure

Nuance's organizational structure provides a framework within which its objectives are planned, executed, controlled, and monitored. Significant aspects of establishing an effective organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Nuance executive management has ultimate responsibility for defining these areas of authority and responsibility and for establishing reporting relationships and authorization protocols. The executive and organizational structure, lines of authority, reporting, and responsibility were summarized above.

Nuance and Microsoft Executive Leadership ensures the organization follows appropriate governance standards.

### Human Resources

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired.

Microsoft employees create individual Core Priorities that align with those of their manager, organization, and Microsoft, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated during one-on-one Connect meetings with their manager. The primary focus of the Connect meetings is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

# Information and Communication

Nuance Healthcare maintains internal SharePoint and Confluence sites that are populated with detailed application, architecture and system information and processes providing employees with ready access to information on application system functions, implementation, and operation.

Ticketing systems provide a record and notification basis of changes, Customer Service Center recorded issues, and incidents.

Internal email is also used to communicate time-sensitive information regarding security and system availability, notifying key personnel in the event of problems. External emails are used to inform customers of issues, changes, and updates to product functionality.

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Policies are in place that establish information policies with clear responsibility for the quality of information used to communicate operational, financial, and compliance-related information that makes it possible to run and control the business. These policies deal with not only internally generated data, but also information about external events, activities, and conditions, such as security incidents, necessary to inform business decision making and external reporting.

Effective communication throughout the Company is imperative. Personnel receive a clear message from top management that control responsibilities must be taken seriously. Personnel understand their own role in the internal control system, as well as how individual activities relate to the work of others. Personnel have a means of communicating significant information upstream. There also is effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

### Internal Communications

Nuance has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities and ensure that significant events are communicated. These methods include training new employees on Company policy and commitments, security awareness training for employees, all-hands employee meetings, and the use of email and internal collaboration tools to communicate time-sensitive information.

### External Communications

Nuance has also implemented various methods of communication to help ensure that customers understand Nuance's role and responsibilities in processing customer transactions and ensure that significant events are communicated in a timely manner. These methods include the use of email and Nuance's customer contact line to communicate time-sensitive information.

Nuance utilizes its public-facing website to communicate relevant information regarding the design and operation of the Dragon Medical One and Dragon Medical SpeechKit, as well as Nuance's commitments to external customers. The website also features a portal where customers can communicate with Nuance for system support or to report any incidents or concerns related to the operation or security of the systems.

## Risk Assessment and Mitigation

Information Security Risk Management (ISRM) is a formal and repeatable method for identifying information security risks, determining risk impact and likelihood, and implementing security controls that are appropriate and justified by the risk. Nuance ensures that information (including customer) remains protected from a loss of:

- Confidentiality: information will be accessible only to authorized individuals.
- Integrity: the accuracy and completeness of information will be maintained; and
- Availability: information will be accessible to authorized users and processes when required.

As part of the Information Security Risk Management process, when a risk is identified (e.g., audit finding), it should be logged and assessed with an understanding of:

- Nuance business processes.
- The impact on Nuance assets:
  - The dependency of any business processes.
  - The value of the asset to Nuance or to Nuance customers.
  - The criticality of the asset to Nuance or to Nuance customers.
- The technical systems in place supporting Nuance business.
- The legislation, regulation, and/or compliance requirements to which Nuance is subject.
- Existing security policy exceptions.

Identified risks will be assigned to an owner, logged, and managed using a risk-module tracking tool.

If the decision is to mitigate a risk, additional activities or controls will be identified and implemented via a risk treatment plan which is documented by the Asset Owner and/or risk owner. Any identified "accepted" risks will be evaluated at least annually, and informed decisions will be made in relation to the risk treatment.

The InfoSec and Operational teams are responsible for identifying risks that threaten the achievement of security, availability, and confidentiality. Leadership and management have implemented a process for identifying, analyzing, and addressing relevant risks and aligning the risks with the annually developed organizational strategy and objectives.

### Risk Identification

Nuance has considered significant interactions between itself and relevant external parties and the risks that could affect the Company's ability to provide reliable service to its user entities. Key members of the Executive Management and Operational teams meet annually to identify and review risks to the systems. These discussions culminate in the creation of a comprehensive annual risk assessment that includes formal mitigation strategies for risks beyond Nuance's acceptable thresholds. Other inputs into these risk discussions are the potential impacts of developing technologies, the constantly changing landscape of regulatory and legislative requirements, and the annual reviews of the operating effectiveness of key controls. These risks are documented in a Company wiki.

### Risk Factors

Management considers risks that can arise from both external and internal factors, including those described below.

- External factors
  - Technological developments
  - Changing customer needs or expectations
  - Competition that could alter marketing or service activities
  - New legislation and regulation that could force changes in policies and strategies
  - Natural catastrophes that could lead to changes in operations or information systems
  - Economic changes that could have an impact on management decisions
- Internal factors
  - Significant changes in policies, processes, or personnel
  - Types of fraud, fraud incentives, pressures, opportunities, attitudes, and rationalizations for employees
  - A disruption in information systems processing
  - The quality of personnel hired and methods of training utilized
  - Changes in management responsibilities

### Risk Analysis

Risk analysis is an essential process to the Company's success. It includes the identification of key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves a judgment based on assumptions about the risk and a reasonable analysis of the costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring and to identify the control activities necessary to mitigate the risk. Management identifies these control activities and documents them.

Management reviews the assessed risk levels annually and documents the risk assessment in the annual risk program.

### Potential for Fraud

Management considers the potential for fraud when assessing the risks to Nuance’s objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts, such as violations of governmental regulations.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. The risk assessment is performed annually and considers the potential for fraud.

### Risk Mitigation

Policies and procedures are in place to guide personnel in risk mitigation activities. Nuance has developed monitoring processes as well as policies, procedures, and communications to meet the Company’s objectives during response, mitigation, and recovery efforts. Security stakeholders perform a risk assessment annually that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on a business impact analysis during the annual risk assessment process. The organization maintains insurance to offset the financial impact of a risk materializing.

A third-party management standard is in place that addresses the following:

- Specific requirements for a vendor and business partner
- Due diligence process prior to accepting new vendors or business partners
- Monitoring process to review vendor and business partner compliance
- Termination of contract

The Supplier Risk Management Standard is reviewed and updated annually and on an ad-hoc basis as needed.

Vendors are evaluated in accordance with Microsoft’s processes and are approved by management prior to receiving access to customer data. Nondisclosure agreements for confidentiality and data protection are required to be signed before information designated as confidential can be shared with third parties.

## Monitoring

The Regulated Industries Security Office has defined the Nuance Security Policy to provide management direction and support for information security in accordance with business requirements, relevant laws, and regulations. The Regulated Industries Security Office develops and maintains this policy and publishes it to all internal employees and contractors.

Nuance has a dedicated security team responsible for managing information security and for providing a control self-assessment, mitigation of threats, monitoring and addressing of vulnerabilities, and monitoring overall change for security impact. The security team has put in place an extensive set of policies and standards.

### System Monitoring (Critical Availability Item)

The SRE teams use a variety of utilities including Prometheus, Grafana, Azure Monitor, Idera SQL Diagnostic Manager, scanning tools, and native component monitoring capabilities to identify and detect possible operational anomalies and incidents. The information reported by these tools includes such items as loading and resource utilization, failover, ping response, and notifications of other exceptional system events. Alerts are reviewed by the Site Reliability Center staff and by security and SRE. Critical alerts result in the automatic creation of an incident ticket in the ServiceNow or Remedyforce system. Upon review, they may be entered into the Critical Incident Management system.

Dragon Medical One and Dragon Medical SpeechKit Key Performance Indicators (KPIs) are available for viewing continuously through an online dashboard. These metrics, including resource utilization and capacity indicators to identify issues and plan for increased or changing capacity needs. Resulting change requests drive system updates to support increased capacity or to address other issues.

The Security Information and Event Management (SIEM) product, Microsoft Sentinel, has been implemented. Sentinel provides continuous data collection and log aggregation from all systems/applications. The aggregated data enables incident detection and provides sources for post incident analysis and recovery. The SIEM dashboards are monitored by the Security Intelligence and Operations Center based in India and the United Kingdom, and accessibility by the security leadership team in Burlington, MA.

### Subservice Organization Monitoring

Data center space, power, communications connections, HVAC, and physical security services for the Dragon Medical One and Dragon Medical SpeechKit applications are provided by:

- Microsoft Azure North America East Central U.S. - Ashburn, VA
- Microsoft Azure North America North Central U.S. - Chicago, IL
- Microsoft Azure North America West US 2 - Quincy, WA
- Microsoft Azure North America Canada East - Quebec
- Microsoft Azure North America Canada Central – Toronto
- Microsoft Azure Germany North – Berlin
- Microsoft Azure Germany West Central – Frankfurt

Although controls relating to physical security and implemented by the data center facilities are included in the overall Healthcare control environment specification, these and other services summarized above as provided by the data center vendor are treated as carve-out services.

Management of Nuance Healthcare receives and reviews the SOC 2 Type 2 report of the subservice organization on an annual basis. In addition, through its daily operational activities, management of Nuance Healthcare monitors the services performed by Microsoft Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to subservice organization management.

The services provided by the Subservice Organization are monitored as part of day-to-day operations. As it becomes available, Nuance personnel receive and review documentation provided by the Subservice Organization (e.g., SOC reports, security certifications) to help ensure that security practices are being followed.

## Control Activities

An entity's organizational structure provides a framework within which its objectives are planned, executed, controlled, and monitored. Significant aspects of establishing an effective organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Nuance executive management has ultimate responsibility for defining these areas of authority and responsibility and for establishing reporting relationships and authorization protocols. The executive and organizational structure, lines of authority, reporting, and responsibility were summarized above.

Nuance and Microsoft Executive Leadership ensures the organization follows appropriate governance standards.

Nuance control activities are defined through its established policies and procedures. Policy statements are documented and communicated through various communication methods within Nuance. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action. A list of policies and procedures is documented in the above Procedures section.

### Logical Access

The Global Technology Solutions (GTS) Access Provisioning Process is a formal process for establishing and limiting staff access to Nuance Healthcare GTS systems. Employees are granted logical access to in-scope systems based on system documented requests that are reviewed and approved by appropriate management personnel.

In accord with the GTS Access Termination Process, the Human Resources department provides GTS with notification of employee termination. GTS disables the associated user id and revokes the associated access privileges. The changes are documented in the request system.

Initial guidelines for role-based access control have been developed and are captured in the GTS Role-Based Access Control (RBAC) Guidelines document. RBAC will be implemented as is feasible and appropriate but is dependent on the complex task of coordinating and defining consistent role definitions.

Administrative access to Active Directory, UNIX/Linux servers, VMware servers, databases, storage, and network devices is restricted to authorized employees and is managed with the GTS Access Provisioning Process. Account sharing is not allowed, with the exception of some generic "root" type accounts whose use is minimized. User identities are audited quarterly.

Policies and mechanisms require unique user identification numbers, names, and passwords for authentication of all GTS staff. Password constraints are as follows:

- Passwords have a minimum of 8 characters, including 2 non-alphanumeric characters.
- Passwords expire every 90 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after five failed log-on attempts.
- The last 10 passwords cannot be reused.

### System Operations

#### Incident Management

Nuance Healthcare has a formalized Critical Incident Management process in place. Customers or internal staff/functions can identify potential issues which are vetted against incident criteria defined by the Critical Incident Management Process, and if found to meet the criteria result in the Critical Incident Manager opening an incident. The Manager records the incident, reviews it with management and technical staff, and coordinates resolution actions which most likely result in the creation of change tickets. The Incident

Manager is the responsible authority for coordinating communication, resolution actions and eventual closure.

### Change Management

For Dragon Medical One and Dragon Medical SpeechKit, a set of customer administrators and their privileges are defined as part of the initial customer configuration by the Nuance Healthcare Provisioning Services group. That configuration is then implemented in production by GTS Development Operations in accord with the GTS Change Management Process. Dragon Medical One and Dragon Medical SpeechKit are transactional systems, and service access is gated by customer licenses as validated by the Nuance Management Server (NMS). NMS provides a wide range of product configuration, security and management options. Customer administrators are configured for NMS, and they utilize it to define organizations and users of various types, allocate licenses (both individual and organizational), establish speech processing options, backup, reporting, etc. When users are registered in the system, they are associated with a license which enables their access to Dragon Medical One and Dragon Medical SpeechKit.

Nuance Healthcare has formalized change management in place, as defined by the GTS Change Management Process document. The process requires identification and recording of changes in the request tracking system, review and assessment of risk and potential impact of proposed changes, approval of proposed changes, testing of changes to verify operational functionality, and communication of change nature and status throughout the process. Proposed changes are evaluated to determine if they present a security or other operational risk and what mitigating actions, including employee and customer entity notifications, must be performed. All changes must have back out plans specified. The SRE Change Advisory Board (CAB) management team meets weekly to review and schedule changes to the GTS environments. Emergency changes follow the formal change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented. Changes to infrastructure and software are developed and tested in separate development or test environments before implementation. Developers are not permitted to implement changes independently or alter production environments.

### Availability

Dragon Medical One and Dragon Medical SpeechKit critical data is held in NMS MS SQL Server databases and geo-replicated to the alternate centers. Only five seconds of data loss is expected for NMS SQL data if a failover is required. Dragon Medical Server (DMS) SQL databases and multiple file shares also containing data are replicated three times in each data center. The file shares are also replicated to a secondary file share which also has three replicas. SAS SQL data and file shares are not geo-replicated to the alternate data center as they do not contain critical data. A full backup of SQL database history is performed weekly, snapshots are taken hourly, and transaction logs are saved every two minutes. Active Directory data is replicated and synched between all data centers where DMO is deployed. Access to all data including replicas and backups is restricted to authorized personnel.

Since the Azure sites and the Dragon Medical One and Dragon Medical SpeechKit instances are all active, at any point in time, customers can be directed to an alternate center. In the case of interruption of full service at the primary site, the critical component requiring failover to the alternate is the NMS SQL database, and the only associated impacted functionality is voice-command processing. Dictation processing continues, depending on the version of the customer client, either after a retry or automatically, with minimal customer disruption.

The required actions to make an alternate center a full primary are to make the NMS SQL database at the operational site the primary and to update connection parameters. The NMS SQL database at the alternate site contains current data through the geo-replication process. All other data can be recreated dynamically, if necessary. Failover/failback and recovery scenarios have been successfully tested. Full failover can be completed within five minutes. Customer dictation support, except voice-command processing, is available during the failover operation.

### Confidentiality

The following data categories are associated with the Dragon Medical One and Dragon Medical SpeechKit product. Nuance Healthcare applications are source systems that may, or may not, feed into Customers' Electronic Health Records. Thus, Nuance is subject to HIPAA as a Business Associate of its customers. While much audio and associated text data is retained, it is only used to refine the speech-to-text or other analytic models. Data flows are described in the product architecture and infrastructure overview sections.

- Customer Information - user account, licensing, configuration information - stored in an NMS MS SQL Server database
- Speech profiles – personalized settings that enhance the accuracy and efficiency of speech recognition system. - stored in Azure file system
- Persisted audio and text files, including PHI – audio recordings and text transcripts that are persistently stored - stored in a file system
- Server images – virtual machine snapshots or disk images – stored in Azure backup services
- Server configuration information – stored details that define how a server is setup and operates – stored in Azure DevOps managed repositories and the Ansible platform
- Code base (includes vendor software/firmware, associated licenses, and developed application product code) – stored in Azure DevOps managed repositories

# User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities should have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities should only grant access to the Company's system to authorized and trained personnel.
- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.

- User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
- User entities are responsible for providing capacity forecasts to Nuance.

# Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses Microsoft Azure as a subservice organization for data center colocation services. The Company's controls related to Dragon Medical One and Dragon Medical SpeechKit cover only a portion of the overall internal control for each user entity of Dragon Medical One and Dragon Medical SpeechKit. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of Microsoft Azure.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at the Subservice Organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The Subservice Organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The Subservice Organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the Subservice Organizations' SOC 2 Type 2 report annually. In addition, through its operational activities, Company management monitors the services performed by the Subservice Organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to the Subservice Organizations' management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Dragon Medical One and Dragon Medical SpeechKit to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at Microsoft Azure as described below.

| Criteria | Complementary Subservice Organization Controls |
|---|---|
| CC2.3 | • Azure is responsible for monitoring of critical vendors in their control. |
| CC6.4 | • The Microsoft Azure Facilities are responsible for restricting data center access to authorized personnel.<br>• The Microsoft Azure Facilities are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel. |
| CC6.5<br>CC6.7 | • The Microsoft Azure Facilities are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for their cloud hosting services where Nuance systems reside.<br>• The Microsoft Azure Facilities are responsible for securely decommissioning and physically destroying physical production assets in its control. |

| Criteria | Complementary Subservice Organization Controls |
|---|---|
| CC6.5<br>C1.2 | • The Microsoft Azure Facilities purge or destroy electronic information containing confidential information when they are no longer used. |
| CC7.2<br>A1.2 | • The Microsoft Azure Facilities are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers.<br>• The Microsoft Azure Facilities are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).<br>• The Microsoft Azure Facilities are responsible for overseeing the regular maintenance of environmental protections at data centers. |

# Complementary Corporate-Level Controls

The Company uses Microsoft Azure for a wide variety of services including data center colocation services, HR functions, and vendor management services. The Company's controls related to Dragon Medical One and Dragon Medical SpeechKit cover only a portion of the overall internal control for each user entity of Dragon Medical One and Dragon Medical SpeechKit. The description does not extend to the colocation services, HR functions, or vendor management services provided by Microsoft Azure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of Microsoft Azure.

Although the complementary corporate-level controls at Microsoft Azure have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by the complementary corporate-level controls at Microsoft Azure. For example, complementary corporate-level controls are expected to be in place at Microsoft Azure, related to physical security and environmental protection. Microsoft Azure's physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Nuance management receives and reviews the Microsoft Azure SOC 2 Type 2 reports annually. In addition, through its operational activities, Nuance management monitors the services performed by Microsoft Azure to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to Microsoft Azure.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Dragon Medical One and Dragon Medical SpeechKit to be achieved solely by Nuance. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related controls expected to be implemented at Microsoft Azure as described below.

| Criteria | Complementary Corporate-Level Controls |
|---|---|
| CC1.1 | • Microsoft Azure is responsible for providing the Microsoft Standards of Business Conduct and security policy to new employees and collecting acknowledgments.<br>• Microsoft Azure is responsible for providing confidentiality agreements to new employees and collecting signed agreements.<br>• Microsoft Azure is responsible for the completion of background checks for new employees and contractors. |

| Criteria | Complementary Corporate-Level Controls |
|---|---|
| CC1.2<br>CC1.3 | • Microsoft Azure is responsible for the board of directors meeting annually, maintaining formal meeting minutes, and including directors that are independent of the Company.<br>• Microsoft Azure is responsible for documenting the oversight responsibilities relative to internal control for the board of directors. |
| CC1.4<br>CC2.2 | • Microsoft Azure is responsible for employees completing security awareness training upon hire and annually thereafter.<br>• Microsoft Azure is responsible for managers completing performance appraisals for direct reports annually. |
| CC1.5 | • Microsoft Azure is responsible for documenting disciplinary actions in a formalized sanctions policy. |
| CC6.2<br>CC6.3<br>CC6.5<br>CC6.6 | • Microsoft Azure is responsible for managing logical access to the underlying network, virtualization management, security, and storage devices for its cloud-hosting services where the Nuance applications reside.<br>• Microsoft Azure is responsible for creating and tracking access modification tickets based on quarterly access reviews. |
| CC4.1<br>CC4.2<br>CC9.2 | • Microsoft Azure is responsible for reviewing the attestation reports for critical vendors. |

## Specific Criteria Not Relevant to the System

There were no specific security availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* that were not relevant to the system as presented in this report.

## Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how Dragon Medical One or Dragon Medical SpeechKit were used to provide the service from May 1, 2024 to April 30, 2025.

## Report Use

The description does not omit or distort information relevant to Dragon Medical One or Dragon Medical SpeechKit while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs.

# Section 4

# Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

## Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, Policies and Procedures.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Nuance's organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

## Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period May 1, 2024 to April 30, 2025. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Nuance's Dragon Medical One and Dragon Medical SpeechKit and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

# Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

## Control Environment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| CC1.1 | The entity demonstrates a commitment to integrity and ethical values. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| CC1.2 | The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| CC1.3 | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | An organization chart is documented and defines the organizational structure and reporting lines. | Inspected the organization chart to determine that it was documented and defined the organizational structure and reporting lines. | No exceptions noted. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment. | Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment. | No exceptions noted. |

**Control Environment**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| **CC1.4** | The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| **CC1.5** | The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |

## Information and Communication

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **CC2.1** | The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | |
| | Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution. | Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution. | No exceptions noted. |
| | Internal and external network vulnerability scans are performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans. | Inspected remediation plans for vulnerabilities identified during the sampled quarterly internal and external network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans. | No exceptions noted. |
| | A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur. | Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred. | No exceptions noted. |

## Information and Communication

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | The security owner subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies and security on the production systems. | Inspected example security bulletins and email alerts subscribed to by the security owner to determine that the security owner subscribed to industry security bulletins and email alerts and used them to monitor the impact of emerging technologies and security on the production systems. | No exceptions noted. |
| | A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production systems, and the system administrators review the changes for appropriateness. | Inspected FIM tool alert configurations and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems. | No exceptions noted. |
| | | Inspected review documentation for a sample of potential unauthorized changes to the production systems to determine that the system administrators were required to review the changes for appropriateness when alerted by the FIM tool. | No exceptions noted. |
| **CC2.2** | The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment. | Inspected the information security policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment. | No exceptions noted. |

## Information and Communication

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| | System changes are communicated to authorized internal users. | Inspected tickets for a sample of system changes to determine that system changes were communicated to authorized internal users. | No exceptions noted. |
| | A formalized ethics and compliance policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns. | Inspected the formal ethics and compliance policy to determine that a formalized ethics and compliance policy was established and an anonymous communication channel was available for employees to report potential security issues or fraud concerns. | No exceptions noted. |
| **CC2.3** | The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
| | Customer Hosted Service Agreements and Hosted Service Orders include the communication of the Company's commitments to its customers. | Inspected the Hosted Service Agreement and Hosted Service Order templates to determine that the Company's commitments were communicated to customers. | No exceptions noted. |
| | Formal information sharing agreements are in place with critical vendors. These agreements include commitments from third parties to report actual or suspected security events and incidents to the Company. | Inspected critical vendor review documentation to determine that formal information sharing agreements were in place with critical vendors to report actual or suspected security events and incidents to the Company. | No exceptions noted. |

| Information and Communication | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Release notes for changes that affect the system are documented and communicated to internal and external users. | Inspected release note communication for a sample of changes to determine that release notes were documented and communicated to internal and external users for implemented changes that affected the system. | No exceptions noted. |
| | An external-facing support system is in place that allows users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | Inspected the customer reporting portal to determine that an external-facing support system was in place that allowed users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | No exceptions noted. |
| | Guidelines and technical support resources related to system operations are provided on the Company's website. | Inspected the Company's website to determine that guidelines and technical support resources related to system operations were provided on the Company's website. | No exceptions noted. |
| | An external-facing status webpage is used to document and communicate current information on service availability to internal and external users. | Inspected the external-facing website to determine that an external-facing status webpage was used to document and communicate current information on service availability to internal and external users. | No exceptions noted. |

## Risk Assessment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **CC3.1** | The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | |
| | The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives. | Inspected documentation from the risk assessment performed during the period to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives. | No exceptions noted. |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| **CC3.2** | 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. | | |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |

## Risk Assessment

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually. | Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions. | No exceptions noted. |
| | | Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| **CC3.3** | The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC3.4** | The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| | A configuration management tool (CMT) is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected CMT configurations to determine that a CMT was in place to ensure that system configurations were deployed consistently throughout the environment. | No exceptions noted. |
| | Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test. | No exceptions noted. |

## Monitoring Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| **CC4.1** | The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | |
| | Elements of the Company’s control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution. | Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution. | No exceptions noted. |
| | Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test. | No exceptions noted. |
| | Internal and external network vulnerability scans are performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |

## Monitoring Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans. | Inspected remediation plans for vulnerabilities identified during the sampled quarterly internal and external network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans. | No exceptions noted. |
| **CC4.2** | 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. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution. | Inspected the control self-assessment documentation to determine that control self-assessments were performed by management during the period to gain assurance that controls were in place and operating effectively and corrective actions were taken by management based on relevant findings and tracked to resolution. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC5.1** | The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | |
| | As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks. | Inspected documentation from the risk assessment performed during the period to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks. | No exceptions noted. |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| **CC5.2** | The entity also selects and develops general control activities over technology to support the achievement of objectives. | | |
| | As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks. | Inspected documentation from the risk assessment performed during the period to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks. | No exceptions noted. |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

## Control Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **CC5.3** | The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
| | Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access<br>- Restricting access based on separation of duties and least privilege | Inspected system access control procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to perform the following system access control functions:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access<br>- Restricting access based on separation of duties and least privilege | No exceptions noted. |
| | Information security policies and procedures are documented and define the information security rules and requirements for the service environment. | Inspected the Company's information security policies and procedures to determine that they were documented and defined the information security rules and requirements for the service environment. | No exceptions noted. |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |

## Control Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |
| | A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data classification policy to determine that a data classification policy was documented to help ensure that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |
| | Formal procedures that outline requirements for vulnerability management are documented and include the following components:<br>- Methods for identifying vulnerabilities and frequency<br>- Assessing the severity of identified vulnerabilities<br>- Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines<br>- Handling of system components for which no measures are initiated to remediate or mitigate vulnerabilities | Inspected the vulnerability management procedures to determine that formal procedures that outlined requirements for vulnerability management were documented and included the following components:<br>- Methods for identifying vulnerabilities and frequency<br>- Assessing the severity of identified vulnerabilities<br>- Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines<br>- Handling of system components for which no measures are initiated to remediate or mitigate vulnerabilities | No exceptions noted. |

## Control Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Formal policies and procedures that outline the requirements for vendor management are documented and include the following components:<br>- Maintaining a list of critical vendors<br>- Requirements for the assessment of risks resulting from the procurement of third-party services<br>- Requirements for the classification of third parties<br>- Information security requirements for the processing, storage, or transmission of information by third parties<br>- Requirements for dealing with vulnerabilities, security incidents, and malfunctions<br>- Specifications for the contractual agreement and monitoring of third-party vendor requirements<br>- Requirements for critical vendors to maintain their own security practices and procedures<br>- Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment | Inspected the vendor management policy to determine that formal policies and procedures that outlined the requirements for vendor management were documented and included the following components:<br>- Maintaining a list of critical vendors<br>- Requirements for the assessment of risks resulting from the procurement of third-party services<br>- Requirements for the classification of third parties<br>- Information security requirements for the processing, storage, or transmission of information by third parties<br>- Requirements for dealing with vulnerabilities, security incidents, and malfunctions<br>- Specifications for the contractual agreement and monitoring of third-party vendor requirements<br>- Requirements for critical vendors to maintain their own security practices and procedures<br>- Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment | No exceptions noted. |
| | Formal policies and procedures that outline the technical and organizational safeguards for change management of system components are documented and include the following components:<br>- Change management roles and responsibilities<br>- Criteria for risk assessment, categorization, and prioritization of changes<br>- Approvals for implementation of changes<br>- Requirements for the performance and documentation of tests, including rollback plans<br>- Requirements for segregation of duties during development, testing, and release of changes | Inspected the change management procedures to determine that formal policies and procedures that outlined the technical and organizational safeguards for change management of system components were documented and included the following components:<br>- Change management roles and responsibilities<br>- Criteria for risk assessment, categorization, and prioritization of changes<br>- Approvals for implementation of changes<br>- Requirements for the performance and documentation of tests, including rollback plans<br>- Requirements for segregation of duties during | No exceptions noted. |

## Control Activities

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | - Requirements for the implementation and documentation of emergency changes | development, testing, and release of changes<br>- Requirements for the implementation and documentation of emergency changes | |
| | A formal security and software development life cycle (SDLC) methodology is in place that governs the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies. | Inspected security and SDLC documentation to determine that a formal security and SDLC methodology was in place that governed the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies. | No exceptions noted. |
| | Network and system hardening standards are documented based on Center for Internet Security (CIS) Benchmarks and reviewed at least annually. | Inspected network and system hardening standards to determine that they were documented based on CIS Benchmarks and reviewed during the period. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |
| | Policies and procedures derived from the information security policy are documented, version controlled, reviewed at least annually, approved by management, and communicated to authorized users. | Inspected the policies and procedures to determine that policies and procedures derived from the information security policy were documented, version controlled, reviewed during the period, and approved by management. | No exceptions noted. |
| | | Inspected the Company intranet to determine that policies and procedures were communicated to authorized users. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Remote access to production systems is restricted to authorized employees with valid multi-factor authentication (MFA) tokens over an encrypted virtual private network (VPN) connection. | Inspected system configurations and observed a remote login session to determine that remote access to production systems was restricted to authorized employees with valid MFA tokens over an encrypted VPN connection. | No exceptions noted. |
| | Authentication to the following in-scope production system components requires unique usernames and passwords or authorized Secure Shell (SSH) keys:<br>- Network<br>- Applications<br>- Data stores<br>- Microsoft Azure console<br>- Firewalls<br>- Log data | Inspected system configurations and observed login attempts to determine that authentication to the following in-scope production system components required unique usernames and passwords or authorized SSH keys:<br>- Network<br>- Applications<br>- Data stores<br>- Microsoft Azure console<br>- Firewalls<br>- Log data | No exceptions noted. |
| | Passwords for in-scope system components are configured according to the Company's policy, which requires the following (unless there is a system limitation):<br>- Minimum password length 8 characters including 2 non-alphanumeric characters<br>- Max password age of 90 days for non-privileged accounts and 60 days for privileged accounts<br>- Cannot use last 10 passwords<br>- Lockout threshold of 5 incorrect passwords | Inspected the password policy and password configurations for in-scope system components to determine that passwords were configured according to Company policy, which required the following (unless there was a system limitation):<br>- Minimum password length 8 characters including 2 non-alphanumeric characters<br>- Max password age of 90 days for non-privileged accounts and 60 days for privileged accounts<br>- Cannot use last 10 passwords<br>- Lockout threshold of 5 incorrect passwords | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | The network is segmented to prevent unauthorized access to customer data. | Inspected network configurations to determine that the network was segmented to prevent unauthorized access to customer data. | No exceptions noted. |
| | A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged. | Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged. | No exceptions noted. |
| | Encryption is enabled for data stores housing sensitive customer data. | Inspected data store settings to determine that encryption was enabled for data stores housing sensitive customer data. | 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. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process. | Inspected termination checklists and system access logs for a sample of terminated employees to determine that a termination checklist was completed and logical access was revoked within 24 hours of termination as part of the termination process. | No exceptions noted. |
| | | Inspected a listing of terminated employees and compared the listing to the active in-scope system access listings to determine that terminated employees did not retain logical access to the in-scope systems after their separation. | No exceptions noted. |
| | Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. | Inspected access review documentation for a sample of quarters to determine that quarterly access reviews were conducted by management for the in-scope system components to help ensure that access was restricted appropriately. | No exceptions noted. |
| **CC6.3** | The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Privileged access to the following in-scope production system components is restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- Data stores<br>- Microsoft Azure console | Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to the following in-scope production system components was restricted to authorized users with a business need:<br>- Network<br>- Applications | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | - Firewalls<br>- Log data | - Data stores<br>- Microsoft Azure console<br>- Firewalls<br>- Log data | |
| | User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | No exceptions noted. |
| | Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process. | Inspected termination checklists and system access logs for a sample of terminated employees to determine that a termination checklist was completed and logical access was revoked within 24 hours of termination as part of the termination process. | No exceptions noted. |
| | | Inspected a listing of terminated employees and compared the listing to the active in-scope system access listings to determine that terminated employees did not retain logical access to the in-scope systems after their separation. | No exceptions noted. |
| | Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. | Inspected access review documentation for a sample of quarters to determine that quarterly access reviews were conducted by management for the in-scope system components to help ensure that access was restricted appropriately. | No exceptions noted. |

### Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | Access to migrate changes to production is restricted to authorized personnel. Developers must have changes reviewed prior to migration in production. | Inspected system access listings, inquired of management, and compared each user's level of access to their job role to determine that access to migrate changes to production was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected system configurations to determine that developers were required to have changes reviewed prior to migration in production. | No exceptions noted. |
| | Service account login credentials are stored in a password manager, and access to the credentials is restricted to authorized users with a business need. | Inspected the password management tool to determine that service account login credentials were stored in a password manager. | No exceptions noted. |
| | | Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that access to the service account login credentials was restricted to authorized users with a business need. | No exceptions noted. |
| **CC6.4** | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | | |
| | The Company's production environment is hosted at Microsoft Azure, which is carved out for the purposes of this report. | Not applicable. | Not applicable. |
| **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. | | |
| | Elements of the Company's control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |

**Logical and Physical Access Controls**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged. | Inspected the production system asset inventory to determine that a formal inventory of production system assets that included asset owners was maintained and changes to the inventory were logged. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |
| **CC6.6** | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | |
| | Remote access to production systems is restricted to authorized employees with valid multi-factor authentication (MFA) tokens over an encrypted virtual private network (VPN) connection. | Inspected system configurations and observed a remote login session to determine that remote access to production systems was restricted to authorized employees with valid MFA tokens over an encrypted VPN connection. | No exceptions noted. |
| | Firewall rulesets and security groups are used and configured to prevent unauthorized access to the production environment. | Inspected firewall ruleset and security group configurations to determine that firewall rules and security groups were used and configured to prevent unauthorized access to the production environment. | No exceptions noted. |
| | A web application firewall (WAF) is used and configured to prevent unauthorized access to the production environment. | Inspected WAF configurations to determine that a WAF was used and configured to prevent unauthorized access to the production environment. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Firewall rulesets and security groups are reviewed at least annually. Change tickets are created to track any firewall modifications as a result of the review.<br>A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No changes were required as a result of the firewall ruleset or security group reviews, therefore no change tickets were created to track firewall rule or security group modifications resulting from the review performed during the period. | Inspected the firewall and security group review documentation to determine that firewall rulesets and security groups were reviewed during the period. | No exceptions noted. |
| | | Inquired of management and inspected firewall ruleset and security group review documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether change tickets were created to track firewall rule or security group modifications resulting from the review. | Not tested. No changes were identified as required as a result of the firewall ruleset or security group review performed during the period, therefore no change tickets were created to track firewall rule or security modifications resulting from the review. |
| | Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. | Inspected transmission protocol configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | An intrusion detection system (IDS) and intrusion prevention system (IPS) are used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. Alerts are configured to notify administrators to investigate and take appropriate action based on the severity of the alert. | Inspected IDS and IPS configurations to determine that an IDS and IPS were used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. | No exceptions noted. |
| | | Inspected IDS and IPS alert configurations and example alerts to determine that alerts were configured to notify administrators of detected and prevented potential security breaches for investigation and resolution. | No exceptions noted. |

**Logical and Physical Access Controls**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected a sample of patches to the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | 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. | | |
| | Elements of the Company’s control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| | Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. | Inspected transmission protocol configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| **CC6.8** | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives. | | |
| | Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant production servers and endpoints. | Inspected anti-malware software configurations to determine that anti-malware technology was deployed for environments commonly susceptible to malicious attack and was configured to be updated routinely, logged, and installed on all relevant production servers and endpoints. | No exceptions noted. |

## Logical and Physical Access Controls

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | An intrusion detection system (IDS) and intrusion prevention system (IPS) are used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. Alerts are configured to notify administrators to investigate and take appropriate action based on the severity of the alert. | Inspected IDS and IPS configurations to determine that an IDS and IPS were used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. | No exceptions noted. |
| | | Inspected IDS and IPS alert configurations and example alerts to determine that alerts were configured to notify administrators of detected and prevented potential security breaches for investigation and resolution. | No exceptions noted. |
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected a sample of patches to the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

## System Operations

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Internal and external network vulnerability scans are performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans. | Inspected remediation plans for vulnerabilities identified during the sampled quarterly internal and external network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans. | No exceptions noted. |
| | A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| | A configuration management tool (CMT) is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected CMT configurations to determine that a CMT was in place to ensure that system configurations were deployed consistently throughout the environment. | No exceptions noted. |

## System Operations

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur. | Inspected the log management tool configurations to determine that a log management tool was utilized to identify trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when specific events occurred. | No exceptions noted. |
| | Internal and external network vulnerability scans are performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans. | Inspected remediation plans for vulnerabilities identified during the sampled quarterly internal and external network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans. | No exceptions noted. |
| | An intrusion detection system (IDS) and intrusion prevention system (IPS) are used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. Alerts are configured to notify administrators to investigate and take appropriate action based on the severity of the alert. | Inspected IDS and IPS configurations to determine that an IDS and IPS were used to provide continuous monitoring of the Company's network and early detection and prevention of potential security breaches. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | | Inspected IDS and IPS alert configurations and example alerts to determine that alerts were configured to notify administrators of detected and prevented potential security breaches for investigation and resolution. | No exceptions noted. |
| | An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected the infrastructure monitoring tool configurations and example alerts to determine that an infrastructure monitoring tool was utilized to monitor system or infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| | Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test. | No exceptions noted. |
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected a sample of patches to the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

**System Operations**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | Security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives. | Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the Company's security incident response policies and procedures. | No exceptions noted. |
| | Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the annual penetration test. | No exceptions noted. |

## System Operations

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Internal and external network vulnerability scans are performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed at least quarterly to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans. | Inspected remediation plans for vulnerabilities identified during the sampled quarterly internal and external network vulnerability scans to determine that remediation plans were developed and changes were implemented to remediate all critical and high vulnerabilities identified during the scans. | No exceptions noted. |
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected a sample of patches to the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | 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. | | |
| | Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |

**System Operations**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents. | Not tested. No security incidents were identified during the period. |
| **CC7.5** | The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
| | Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually. | Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions. | No exceptions noted. |
| | | Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| | Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |

**System Operations**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents. | Not tested. No security incidents were identified during the period. |
| | The incident response plan is tested at least annually to assess the effectiveness of the incident response program. | Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program. | No exceptions noted. |

## Change Management

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| **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. | | |
| | Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected change request tickets for a sample of software and infrastructure changes to determine that software and infrastructure changes were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | Access to migrate changes to production is restricted to authorized personnel. Developers must have changes reviewed prior to migration in production. | Inspected system access listings, inquired of management, and compared each user's level of access to their job role to determine that access to migrate changes to production was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected system configurations to determine that developers were required to have changes reviewed prior to migration in production. | No exceptions noted. |
| | Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. | Inspected a sample of patches to the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

## Risk Mitigation

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | |
| | A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| | Security incident response policies and procedures are documented and provide guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | The incident response plan is tested at least annually to assess the effectiveness of the incident response program. | Inspected the incident response plan test results to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program. | No exceptions noted. |
| | Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually. | Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions. | No exceptions noted. |
| | | Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |

## Risk Mitigation

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other Company data centers in the event of the loss of a facility. | Inspected multi-location deployment configurations to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other Company data centers in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to a secondary data center or secondary availability zone in real time. Alerts are configured to notify administrators if replication fails. | Inspected database configurations and monitoring dashboards to determine that databases were replicated to a secondary data center or secondary availability zone in real time and alerts were configured to notify administrators if replication failed. | No exceptions noted. |
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | | |
| | Elements of the Company’s control environment are performed by Microsoft Azure, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |

## Additional Criteria for Availability

**Availability**

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| **A1.1** | The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | |
| | System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand. | Inspected auto-scaling configurations and configurations of system capacity evaluation to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand. | No exceptions noted. |
| | An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected the infrastructure monitoring tool configurations and example alerts to determine that an infrastructure monitoring tool was utilized to monitor system or infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| **A1.2** | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. | | |
| | Hourly differential and weekly full backups are configured for data stores housing sensitive customer data. Alerts are configured to notify administrators of failed backups for investigation and resolution.<br>A portion of this control did not operate during the period. No backup failures occurred. | Inspected backup configurations to determine that hourly differential and weekly full backups were configured for data stores housing sensitive customer data. | No exceptions noted. |
| | | Inspected backup failure alert configurations and example alerts to determine that alerts were configured to notify administrators of failed backups. | No exceptions noted. |

## Availability

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor's Tests | Results of Tests |
|---|---|---|---|
| | | Inquired of management and inspected backup documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether backup failures were investigated and resolved. | Not tested. No backup failures were identified during the period. |
| | Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually. | Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions. | No exceptions noted. |
| | | Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other Company data centers in the event of the loss of a facility. | Inspected multi-location deployment configurations to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other Company data centers in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to a secondary data center or secondary availability zone in real time. Alerts are configured to notify administrators if replication fails. | Inspected database configurations and monitoring dashboards to determine that databases were replicated to a secondary data center or secondary availability zone in real time and alerts were configured to notify administrators if replication failed. | No exceptions noted. |

## Availability

| TSC Reference | Trust Services Criteria and Applicable Control Activities | Service Auditor’s Tests | Results of Tests |
|---|---|---|---|
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |
| **A1.3** | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | |
| | Data backup restoration tests are performed at least annually to verify data reliability and information integrity. | Inspected the data backup restoration test results to determine that data backup restoration tests were performed during the period to verify data reliability and information integrity. | No exceptions noted. |
| | Business continuity and disaster recovery (BC/DR) plans are documented to support continuity and recovery of critical services and business processes after unexpected business interruptions. BC/DR roles and responsibilities have been assigned to appropriate individuals, and the continuity and recovery of critical services and business processes is based on a strategy approved by senior management. The plans are tested at least annually. | Inspected the BC/DR plans to determine that BC/DR plans were documented to support the continuity and recovery of critical services and business processes after unexpected business interruptions. | No exceptions noted. |
| | | Inspected the BC/DR plans to determine that BC/DR roles and responsibilities had been assigned to appropriate individuals and the continuity and recovery of critical services and business processes was based on a strategy approved by senior management. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected backup and recovery procedures to determine that formal procedures were documented that outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |

## Additional Criteria for Confidentiality

| Confidentiality | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **C1.1** | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | |
| | A data classification policy is documented to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data classification policy to determine that a data classification policy was documented to help ensure that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |
| | Confidential or sensitive customer data is prohibited by policy from being used or stored in non-production systems or environments. | Inspected the data classification policy to determine that confidential or sensitive customer data was prohibited by policy from being used or stored in non-production systems or environments. | No exceptions noted. |
| | | Inspected system configurations and observed the test environment to determine that only test data was used in non-production systems or environments. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |
| **C1.2** | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | |
| | Electronic media containing confidential information is purged or destroyed, and certificates of destruction are issued or evidence of the purging or destruction is retained for each device destroyed. | Inspected certificates of destruction for a sample of purged or destroyed media to determine that electronic media containing confidential information was purged or destroyed and certificates of destruction were issued or evidence of the purging or destruction was retained for each device destroyed. | Carve-out to Azure |

| Confidentiality | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Customer data in the application, metadata, and data stored in data backups are deleted when customers leave the service in accordance with contractual agreements. | Inspected tickets for data removal or purging for a sample of customers who left the service to determine that customer data in the application, metadata, and data stored in data backups were deleted when customers left the service in accordance with contractual agreements. | No exceptions noted. |