Nuance Healthcare

SOC 2 Type 2 Report - Security, Availability, and Confidentiality

Independent Service Auditor's Report on Controls Placed in Operation for Hosted Infrastructure Services for Dragon Medical One

For the Period May 1, 2023 through April 30, 2024

This report is intended solely for use by the management of Nuance Healthcare, user entities of Nuance Healthcare services, and other parties who have sufficient knowledge and understanding of Nuance Healthcare services covered by this report (each referred to herein as a "specified user").

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

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

NUANCE HEALTHCARE

TABLE OF CONTENTS
CONTROLS PLACED IN OPERATION FOR HOSTED INFRASTRUCTURE SERVICES
FOR THE PERIOD MAY 1, 2023 THROUGH APRIL 30, 2024

Pages

7910 WOODMONT AVENUE
SUITE 500
BETHESDA, MD 20814
(T) 301.986.0600

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

To Nuance Healthcare:

Scope

We have examined Nuance Healthcare's accompanying description of its Hosted Infrastructure Services for Dragon Medical One throughout the period May 1, 2023 to April 30, 2024, (description) based on the criteria for a description of a service organization's system set forth in *DC 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, 2023 to April 30, 2024, to provide reasonable assurance that Nuance Healthcare's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA, *Trust Services Criteria*.

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

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

Service Organization's Responsibilities

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

Service Organization's Responsibilities (Continued)

Nuance Healthcare 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 AICPA.

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.

Inherent Limitations (Continued)

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 III, "Criteria, Test of Operating Effectiveness and Results" of this report.

Opinion

In our opinion, in all material respects—

a. the description presents Nuance Healthcare's Hosted Infrastructure Services system that was designed and implemented throughout the period May 1, 2023 to April 30, 2024, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period May 1, 2023 to April 30, 2024, to provide reasonable assurance that Nuance Healthcare's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Nuance Healthcare's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period May 1, 2023 to April 30, 2024, to provide reasonable assurance that Nuance Healthcare's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Nuance Healthcare's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Nuance Healthcare; user entities of Nuance Healthcare's Hosted Infrastructure system during some or all of the period May 1, 2023 to April 30, 2024, business partners of Nuance Healthcare subject to risks arising from interactions with the Hosted Infrastructure Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary 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.

Restricted Use (Continued)

- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks.

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

Councilor, Buchanan + Mitchell, P.C.

Bethesda, Maryland
September 6, 2024

Councilor, Buchanan & Mitchell, P.C.

SECTION I: ASSERTION OF NUANCE COMMUNICATIONS, INC.

We have prepared the accompanying description of Nuance Healthcare's (Nuance's) Hosted Infrastructure Services system titled Dragon Medical One throughout the period May 1, 2023 to April 30, 2024, (description) based on the criteria for a description of a service organization's system set forth in *DC 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 Hosted Infrastructure system that may be useful when assessing the risks arising from interactions with Nuance's Healthcare's Hosted Infrastructure Services system, particularly information about system controls that Nuance Healthcare 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 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 Healthcare uses a subservice organization to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nuance Healthcare, to achieve Nuance Healthcare's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuance Healthcare's, controls the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nuance Healthcare's controls. The description does not disclose the actual controls at the subservice organization.

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

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

1) The description presents Nuance Healthcare's Hosted Infrastructure Services system that was designed and implemented throughout the period May 1, 2023 to April 30, 2024, in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period May 1, 2023 to April 30, 2024, to provide reasonable assurance that Nuance Healthcare's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Nuance Healthcare's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period May 1, 2023 to April 30, 2024, to provide reasonable assurance that Nuance Healthcare's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nuance Healthcare's controls operated effectively throughout that period.

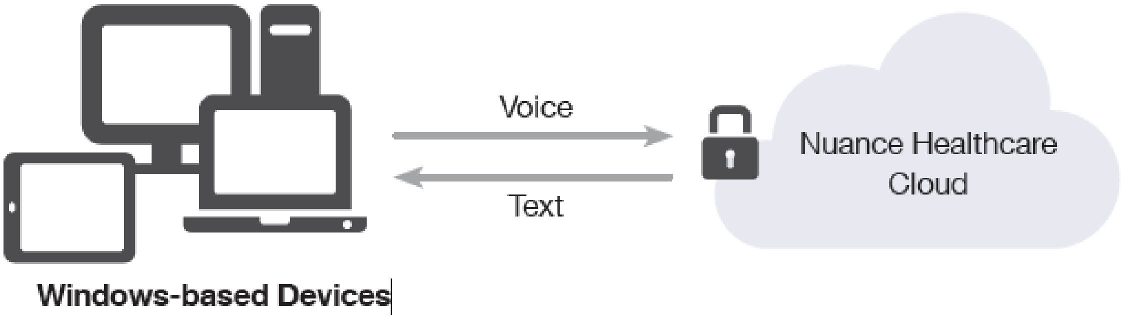
SECTION II: DESCRIPTION OF THE SYSTEM

Description of the Systems Provided by Nuance Healthcare

Nuance Communications, Inc., a Microsoft company, is a leading provider of voice and language solutions for businesses and consumers around the world. Nuance Healthcare leads the market in creating clinical understanding solutions that drive smart, efficient decisions across healthcare. More than 500,000 physicians and 10,000 healthcare facilities worldwide leverage Nuance Healthcare's award-winning, voice-enabled clinical documentation and analytics solutions to support the physician in any clinical workflow and on any device.

Description of Dragon Medical One Services

Dragon® Medical One is 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 provides 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 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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

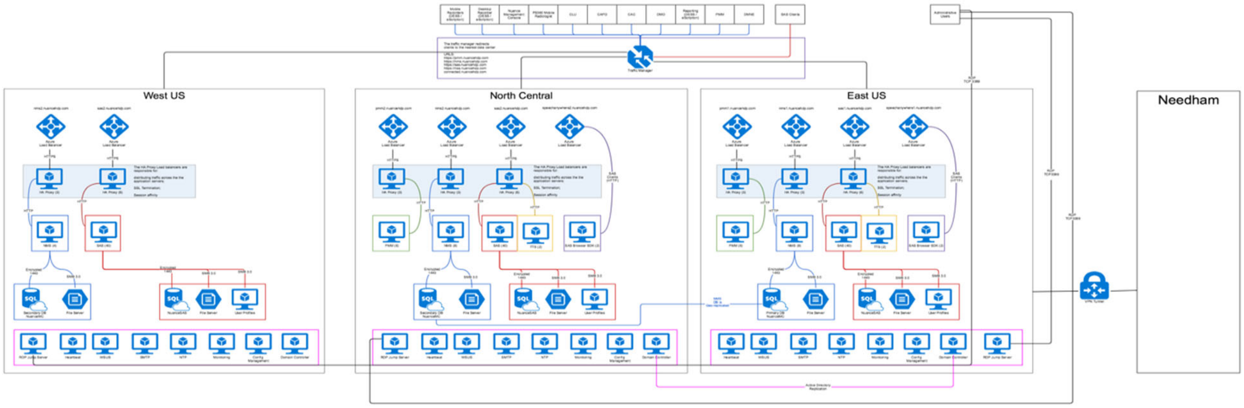
Components of the Dragon Medical One System

Infrastructure and Software

Dragon Medical One is supported by active-active instances at three Microsoft Azure cloud computing data centers providing highly scalable, responsive, and available environments. Customer transactions are dispatched to one of three data centers by Azure traffic management, and traffic loads are balanced across components within each center. The virtualized environments are mirrored at each site and include:

- Web interfaces to the hosted services, virtualized clustered Windows Server 2012 R2 configurations running primarily C# and .NET code;
- Dragon Medical Server (DMS) nodes, virtualized servers running proprietary C code that perform speech to text conversion;
- PowerMic Mobile (PMM) servers, virtualized Windows servers with C# application code, supporting acquisition of audio from PowerMic devices;
- Data services, provided by clustered Azure provisioned MS SQL Server databases;
- Nuance Management Server (NMS) servers, used for license validation, auto-text command processing, and other services. (Transactions are license based and not user based, although users are customer defined and assigned licenses.);
- Administrative servers supporting: Active Directory (AD), monitoring, time services (NTP), configuration management (Salt), eMail, deployment (Jump), general management, e.g., SQL Studio;
- Network security protection leveraging Trend Micro Intrusion Prevention System (IPS) and Intrusion Detection System (IDS);
- Environments for: Production, Development, Staging, and QA.

Captured audio is submitted from the customer application interface via authorized encrypted connections, converted to text, and returned to the customer application.

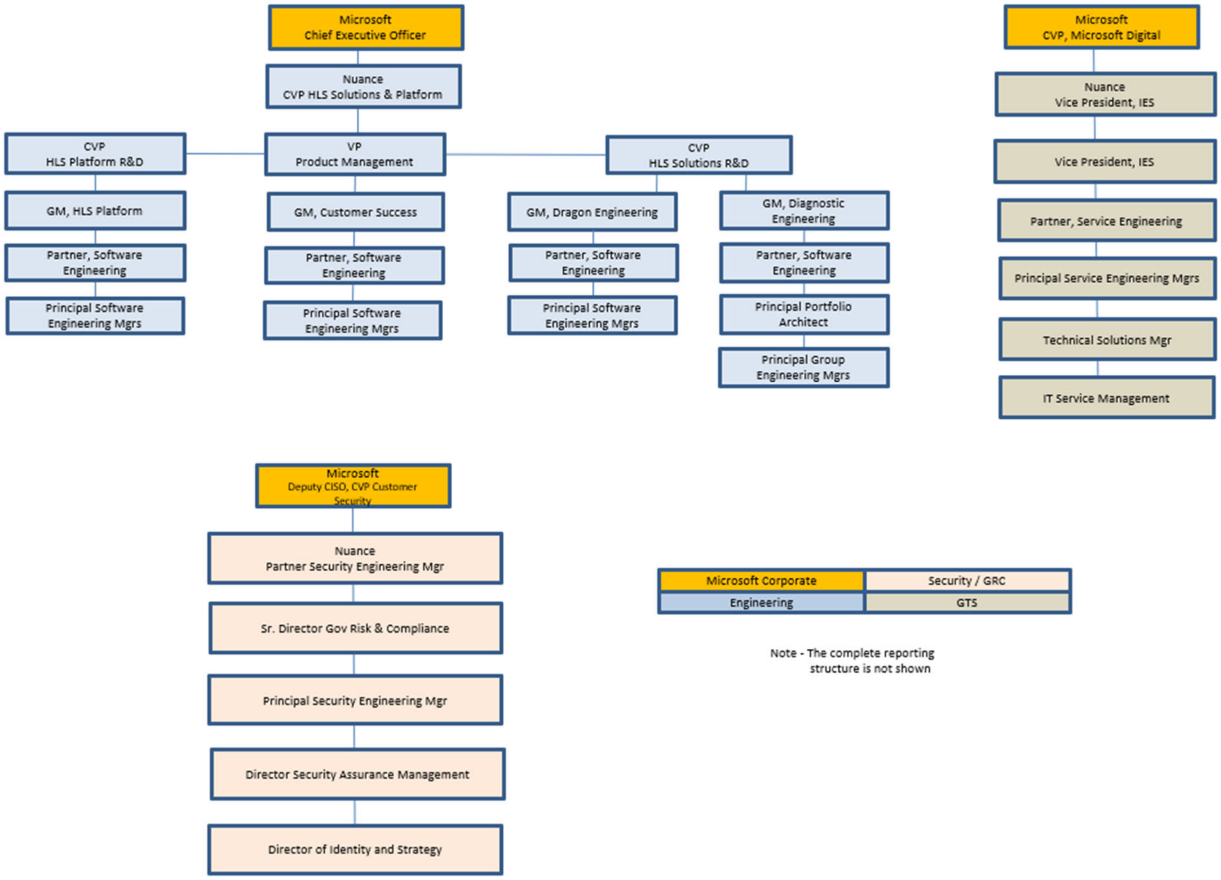


SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Components of the Dragon Medical One System (Continued)

People

Nuance Healthcare is organized into functional areas as depicted in the following diagram and described below. Nuance Healthcare (approximately 2,600 staff) is a business segment of the larger Nuance Communications, Inc. Segments of the Nuance Healthcare organization relevant to the current audit are shown below.


Microsoft Chief Executive Officer
Nuance CVP HLS Solutions & Platform
CVP HLS Platform R&D
VP Product Management
CVP HLS Solutions R&D
GM, HLS Platform
Partner, Software Engineering
Principal Software Engineering Mgrs
GM, Customer Success
Partner, Software Engineering
Principal Software Engineering Mgrs
GM, Dragon Engineering
Partner, Software Engineering
Principal Software Engineering Mgrs
GM, Diagnostic Engineering
Partner, Software Engineering
Principal Portfolio Architect
Principal Group Engineering Mgrs
Microsoft CVP, Microsoft Digital
Nuance Vice President, IES
Vice President, IES
Partner, Service Engineering
Principal Service Engineering Mgrs
Technical Solutions Mgr
IT Service Management
Microsoft Deputy CISO, CVP Customer Security
Nuance Partner Security Engineering Mgr
Sr. Director Gov Risk & Compliance
Principal Security Engineering Mgr
Director Security Assurance Management
Director of Identity and Strategy
Microsoft Corporate
Security / GRC
Engineering
GTS

Note - The complete reporting structure is not shown

- Corporate - Executives, senior operations staff, and company administrative support, such as legal, training, contracting, accounting, finance, and human resources.

Within the Healthcare segment two major groups are relevant for this audit.

- Technical Operations/Support - Staff in this area provides for operational implementation, operation, and support across all of the application products.
  - Technical Operations
    - Product liaison and client executives
    - Customer service center staff supports each product taking customer phone calls, responding to emails, and handling various interactions related to product use, performance, issues, etc.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Components of the Dragon Medical One System (Continued)

People (Continued)

- Professional Services
  - Creates application configurations for new customers to be instantiated in the production environment by GTS Development Operations
- Engineering
  - Staff developing and supporting Healthcare application products
  - Product engineering SRE and the Hosted Infrastructure and Data Center Group, also known as Global Technology Solutions (GTS), implements and supports operation of application environments
    - Project and Asset Management
      - Project Management
      - Business Operations Support
      - Budget/Forecasts
      - Vendor Management
      - Change Management
      - Access Management
      - Quality Assurance
      - Compliance
      - Governance
      - Acquisition
      - Integration
      - Asset Management Program
      - Operations and Process Improvement
        - Metrics and KPI’s
        - Service Assurance Management
        - Rapid Systems Provisioning and Deployment
        - Tools and Automation

SECTION II: Description of the System (Continued)

Components of the Dragon Medical One System (Continued)

People (Continued)

- Development Operations (two groups)
  - Product Relationship Management
  - Deployment - Dev to Ops End to End Delivery
  - Full Stack Systems Development Life Cycle (SDLC) Support
  - Systems, Storage, Network Support for Application Implementation
  - Liaison for OS & Above (Middleware and Applications)
  - Azure Environment
  - Cloud Architecture
  - Patching/Change Support
  - Tier 2 Support
- IT Business Systems Analysis
  - Service Reliability Center (SRC) / Network Operations Center (NOC) providing 24/7 real time monitoring and event coverage via Melbourne and India sites
  - Incident Management
  - Reason for Outage (RFO) Analysis
  - Expansion of Ops Services (e.g., Telco and Network)
- Site Reliability Engineering
  - Database Administration
  - Servers/Server Virtualization
  - Storage
  - Network/Telco
  - Infrastructure Services
    - Active Directory
    - Authentication Services
    - Certificate Management
    - Antivirus
    - Security Infrastructure
    - NTP
    - DNS
    - DHCP
    - Monitoring Infrastructure
    - Load Balancing
    - Terminal Services
    - Telecom

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Components of the Dragon Medical One System (Continued)

People (Continued)

- Patching/Change Support
- Tier 1, 2, and 3 Support
- Data Center Operations
    - Contract Management
    - Expense Analysis
    - Capacity Planning
    - Layer 1 Standards
    - Break/Fix Support
    - Rack and Stack
- Monitoring Architecture
    - Dashboards
    - Tool Integration
    - Log Management

Processes

Processes have been defined and implemented to cover the following key security life cycle areas:

- Personnel hiring, training, and compliance processes
- Performance of annual and ongoing security risk assessments and implementation of associated mitigations
- Authentication/authorization, changes to, and termination of information system access
- Physical security
- Change management process
- Vulnerability and patch management process
- Critical incident management process
- Asset management processes
- Security and system operation monitoring

These processes are described in more detail in the control environment section of this document.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Components of the Dragon Medical One System (Continued)

Data

The following data categories are associated with the Dragon Medical One 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 a NMS MS SQL Server database
- Speech profiles - stored in Azure file system
- Persisted audio and text files, including PHI, stored in a file system
- Server images
- Server configuration information
- Code base (includes vendor software/firmware, associated licenses, and developed application product code)

System Boundaries

This audit is scoped to Nuance Healthcare hosted services in support of the Dragon Medical One product, and specifically those services that are hosted in United States and Canada facilities.

Control Environment

The control environment provides the overall context for all aspects of internal control. Factors such as the organizational structure, ethical values, assignment of authority and responsibility, and management oversight drive effective adoption and execution of control measures.

Organizational Structure, Authority, and Responsibility

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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Integrity and Ethical Values

The effectiveness of controls is based on the integrity and ethical values of the people who create, administer, and monitor them. Nuance Executive Leadership provides the Microsoft Standards of Business Conduct (Trust Code) for its directors, officers and employees. All employees are required to read and acknowledge this Code in writing upon hire, uphold these standards in day-to-day activities, and comply with all applicable policies and procedures. The Code is intended to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- Avoidance of conflicts of interest, including disclosure to an appropriate person or persons identified in this Code of any transaction or relationship that reasonably could be expected to give rise to such a conflict;
- Full, fair, accurate, timely, and understandable disclosure in reports and documents that the Company files with, or submits to, the United States Securities and Exchange Commission (the SEC) and in other public communications made by the Company;
- Compliance with applicable governmental laws, rules and regulations;
- Adherence to all Nuance policies, including but not limited to Foreign Corrupt Trade Practices and Insider Trading policies;
- The prompt internal reporting to an appropriate person or persons identified in this Code of violations of this Code; and
- Accountability for adherence to this Code.

Security Organization and Management

Nuance Global Security has defined the Global Security Framework Policy to provide management direction and support for information security in accordance with business requirements, relevant laws, and regulations. The Global Security Organization 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 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:

- Policies
  - Global Security Framework Policy

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Security Organization and Management (Continued)

This document covers key security areas:

- Organization of Information Security
- Asset Management
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
    - Microsoft's Responsible Use of Technology
    - Nuance Healthcare Security Policy
    - Resiliency - Business Continuity Policy
- Standards
    - Information Classification and Handling Standard
    - Information Security Risk Management Standard
    - Vulnerability Management Standard

Personnel Security

Nuance hiring practices are formalized and performed via a detailed job requisition process. Employees are hired in accord with job descriptions specifying requisite education and experience levels. Background checks are required for all new hires. As noted above, employees are required to read and agree to the Nuance code of conduct. All employees are required to attend annual security, privacy and compliance awareness training covering a number of areas, including procedures and requirements to report security and privacy issues and incidents. Management monitors training compliance. Defined sanctions and processes are in place to address violations of the code of conduct.

Control Environment (Continued)

Physical Security (Critical Availability Item)

Physical security policies, processes, and mechanisms are in place at Microsoft Azure facilities and are stringently enforced at the two SOC 2 Type 2 certified data centers hosting the Dragon Medical One application. The facilities are highly secure with a robust physical environment designed to provide highly available computing infrastructure. The data centers are in compliance with the following requirements:

- Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors.
- Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.
- Physical access to the data center is reviewed quarterly and verified by the data center operations team.
- Physical access mechanisms (e.g., access card readers, biometric devices, man traps, portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
- The data center facility is monitored 24/7 by security personnel.
- Environmental controls have been implemented to protect systems inside the facility, including temperature and HVAC controls, fire detection and suppression systems, and power management systems.

System Account and Access Management

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

In accordance 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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

System Account and Access Management (Continued)

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 three failed log-on attempts.
- The last 10 passwords cannot be reused.

Change Management

For Dragon Medical One, a set of customer administrators and their privileges is 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 is a transactional system, 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 services.

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 GTS 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.

Vulnerability and Patch Management

The GTS Vulnerability Management Process implements a formal structured process for monthly internal and external infrastructure scans to identify vulnerabilities at GTS data centers. Regular monitoring of CERT alerts and HITRUST Monthly threat briefings is another source of vulnerability identification. Finally, vendor patch distributions provide a third input into the vulnerability management process. In all of these cases, owners of the impacted assets are identified, and the identified vulnerabilities are evaluated.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Vulnerability and Patch Management (Continued)

The risk associated with vulnerability is ranked according to its impact including timelines for implementation, and a remediation plan is agreed in joint discussion with asset and product owners, data center staff, management, and the security team. Remediation is implemented and assessed following implementation. Vulnerabilities and their disposition are tracked by the Security Organization.

Nuance Healthcare uses standardized server build checklists and server policy management tools to help secure its servers, implementing only required services and thus reducing the scope of vulnerabilities. Antivirus software (CrowdStrike Falcon Platform) has been installed and activated to detect and protect against malicious code.

Information Security Risk Management

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. In alignment with Information Security best-practices, 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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Information Security Risk Management (Continued)

Nuance teams meet at least quarterly to address, manage, and report on medium/high risks and their corresponding risk treatment plans.

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.

System Monitoring (Critical Availability Item)

The Site Reliability Engineering (SRE) and GTS Site Reliability Center (SRC) 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 RemedyForce system. Upon review, they may be entered into the Critical Incident Management system.

Dragon Medical One Key Performance Indicators (KPIs) are available for viewing continuously through an online dashboard. These metrics, including resource utilization and capacity indicators, are reviewed at monthly meetings by product development, development operations, operations and other key stake holders 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.

Microsoft Sentinel, the Security Information and Event Management (SIEM) product, continuously collects and aggregates data from all systems and applications. This aggregated data helps in incident detection and provides valuable insights for post-incident analysis and recovery. The SIEM dashboards are monitored by the Security Intelligence & Operations Center (SIO) based in the U.S., India, and the United Kingdom, with access available to the security leadership team in Redmond, WA, United Kingdom, and Burlington, MA.

Data Backup and Recovery (Critical Availability Item)

Dragon Medical One critical data is held in NMS MS SQL Server databases. The NMS SQL databases are replicated three times in each data center and are also geo-replicated to the alternate centers. Only five seconds of data loss is expected for NMS SQL data if a fail over 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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Data Backup and Recovery (Critical Availability Item) (Continued)

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 nightly, 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 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.

Asset Management

Nuance Healthcare maintains a complete inventory of hardware assets across all GTS facilities. The inventory is maintained in a Remedy database. Interim asset identification of software assets has been started. A road map has been prepared for the evolution of the Remedy based capabilities, eventually implementing a full Configuration Management database.

Information and Communication Systems

The Nuance policy documents cited above clearly define information security and privacy policies to help ensure that employees understand their individual roles and responsibilities concerning security processing and controls. Employees are required to attend annual security awareness training that refreshes and updates their security skills.

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. Nuance The Voice site contains general corporate information.

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.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

Control Environment (Continued)

Monitoring of the Subservice Organization

Data center space, power, communications connections, HVAC, and physical security services for the Dragon Medical One 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 U.S. 2 - Quincy, WA
- Microsoft Azure North America Canada East - Quebec
- Microsoft Azure North America Canada Central - Toronto

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 vendors will be treated as carve-out services.

Management of Nuance Healthcare receives and reviews the Type 2 SOC 2 report of the subservice organizations 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.

Complementary Subservice Organization Controls

Nuance Healthcare's controls related to the Hosted Infrastructure system cover only a portion of the overall internal control for each user entity of Nuance Healthcare. It is not feasible for the control objectives related to Hosted Infrastructure to be achieved solely by Nuance Healthcare. Therefore, each user entities controls must be evaluated in conjunction with Nuance Healthcare's controls and the related tests and results described in Section III of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below:

- The subservice organization is responsible for maintaining logical security over the servers and other hardware devices upon which the Dragon Medical One application is hosted.
- The subservice organization is responsible for notifying Nuance Healthcare of any security incidents related to security over the servers and other hardware devices upon which the Dragon Medical One application is hosted.
- The subservice organization is responsible for maintaining physical security over its data center in which the servers used to host the Dragon Medical One application are housed.

SECTION II: DESCRIPTION OF THE SYSTEM (CONTINUED)

User Entity Responsibilities

The following list includes controls that Nuance Healthcare assumes its user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

- Customers are responsible for managing compliance with applicable laws/regulations.
- Customers are responsible for ensuring that their users are establishing appropriate controls over the use of their Nuance Healthcare accounts and passwords.
- Customers are responsible for disabling/deleting account access to their Nuance Healthcare services upon employee role change/employee termination.
- Customers are responsible for ensuring that their users follow appropriate security practices while using Nuance Healthcare applications.
- Customers' administrators are responsible for selection and use of their passwords.
- Customers are responsible for ensuring the confidentiality of user IDs and passwords used to access Nuance Healthcare applications.

Entity Controls Testing Spreadsheet

The examination was limited to operation of Dragon Medical One services by Nuance Healthcare HIS. Accordingly, the examination did not extend to any activities or procedures using client devices or in effect at client premises. It is each client auditor's responsibility to evaluate this information in relation to a client entity's internal controls in place in order to obtain an understanding of the internal controls and assess control risk. The portions of the internal controls provided by the client entities and Nuance Healthcare HIS must be evaluated together. If effective client internal controls are not in place, Nuance Healthcare's HIS controls may not compensate for such weaknesses.

The controls presented and examined address the security, availability, and confidentiality trust principles.

Significant Changes during the Review Period

Nuance Healthcare employees transitioned to Microsoft Human Resources as of August 1, 2023.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC1.0	**Common Criteria Related to the Control Environment**		
CC1.1	*COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.*		
CC1.1A	On a quarterly basis, the CEO conducts All Hands Meetings to communicate information to employees regarding the strategy, tone, and operational priorities of the Company.	Inspected minutes of All Hands Meeting.	No exceptions noted.
CC1.1B	Nuance Communications, Inc., maintains a Code of Ethics and is posted for internal and external reference.	Inspected policies regarding ethical values posted on the Company Intranet.	No exceptions noted.
CC1.1C	All personnel are required to read and understand the code of ethics and sign off on the agreement upon hire. Management monitors employees' compliance with Code of Conduct through regular monitoring and review of employee activities.	For a sample of new employees, inspected code of conduct acceptance.	Exception noted. 1 of 53 employees sampled did not have a signed Code of Conduct acceptance on file.
CC1.1D	The Company has contracted with EthicsPoint, a third-party provider, to provide an anonymous mechanism for employees to report improprieties (Whistleblower Hotline). Each complaint is researched and followed up on a timely basis.	Inquired of management about the existence of any policy violations and sanctions implemented as a result of the violations. Viewed the posting of the Whistleblower Hotline on the Company Intranet.	No exceptions noted.
CC1.1E	The Company has an Integrity and Ethical Values policy that is required to be followed by contractors.	Inspected policies requiring contractors and vendor employees to comply with entity security and privacy policies, to protect entity assets, and to be provided with security awareness and training.	Exceptions noted. 2 of 53 employees sampled did not have documentation of the required annual training. One of the two exceptions is located in a European country and unable to provide documentation.
CC1.1F	Annually, Nuance evaluates employee's performance and compensation through goal setting and annual performance reviews which includes alignment against the Company's standards.	Inspected policies and processes for staff performance evaluation. For a sample of employees, determined that annual performance evaluations were conducted.	Exception noted. 1 of 53 employees sampled did not have a performance evaluation during the period.
CC1.2	*COSO Principle 2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*		
CC1.2A	Annually, the Chief Technology Officer (CTO) - review the individual performance of the directors and determines whether they fulfill their responsibilities under the Charter - determine that the CTO and/or Audit Committee members (as applicable) meet the NYSE listing requirements for independence and financial literacy.	Inspected documentation of the CTO constitution, empowerment, responsibilities, and operating procedures.	No exceptions noted.
CC1.2B	The Nuance Chief Technology Officer (CTO) maintains a Charter and Policies and Procedures which outline the CTO's responsibility.	Inspected documentation of the CTO constitution, empowerment, responsibilities, and operating procedures.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC1.3	*COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*		
CC1.3A	A functional organizational structure is in place defining areas of authority, responsibility, and lines of reporting. The structure is documented in current policies and organization charts that are available to all employees on the Company Intranet. Reporting relationships and organization structures are reviewed annually by senior management as part of security organization planning and adjusted as needed based on changing entity commitments and requirements to ensure their continuing suitability, adequacy, and effectiveness.	Inspected policies and organization charts noting specification of authority, responsibility, and lines of reporting, as well as security management review and oversight.	No exceptions noted.
CC1.3B	Each job role has a specific job description that outlines responsibilities for the role.	Inspected hiring policies and processes. Inspected a sample of roles identified in the organization chart and obtained job descriptions to determine whether the descriptions identified the responsibilities and authority for the selected roles.	No exceptions noted.
CC1.3C	Arrangements with third parties are governed through contractual commitments that include Nuance designated personnel for management of the relationship.	Inspected policies requiring contractors and vendor employees to comply with entity security and privacy policies, to protect entity assets and to be provided with security awareness and training. Selected a sample of contract agreements to ensure that contracts are in place.	No exceptions noted.
CC1.4	*COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*		
CC1.4A	Policies are in place defining expectations and requirements of staff competence. Policies and procedures are in place for annual assessments of employee performance.	Inspected hiring policies and processes regarding required staff competence and policies for security and privacy awareness, training, and compliance. For a sample of employees, inspected personnel files to determine whether the candidate's skills, knowledge, and experience meet the requirements of the position, and whether these qualifications were verified and evaluated as part of the hiring or transfer process.	No exceptions noted.
CC1.4B	Employees are required to complete security awareness training when hired and on an annual basis thereafter. Management monitors training compliance.	Inspected the policy for general employee training, annual security awareness training, and recent training materials. For a sample of employees, verified that the employee participated in the required training programs.	Exceptions noted. 2 of 53 employees sampled did not have documentation of the required annual training. One of the two exceptions is located in a European country and unable to provide documentation.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC1.4	*COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (Continued)*		
CC1.4C	Annually, Nuance evaluates employee's performance and compensation through goal setting and annual performance reviews which includes alignment against the Company's standards.	Inspected policies and processes for staff performance evaluation. For a sample of employees, determined that annual performance evaluations were conducted.	Exception noted. 1 of 53 employees sampled did not have a performance evaluation during the period.
CC1.4D	Prior to employment, personnel, including contractors, are subject to background checks.	Inspected background check policies and procedures. For a sample of employees, inspected records to determine whether a background check was performed.	No exceptions noted.
CC1.5	*COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*		
CC1.5A	The Company has contracted with EthicsPoint, a third-party provider, to provide an anonymous mechanism for employees to report improprieties (Whistleblower Hotline). Each complaint is researched and followed up on a timely basis.	Inquired of management about the existence of any policy violations and sanctions implemented as a result of the violations.	No exceptions noted.
CC1.5B	Annually, Nuance evaluates employee's performance and compensation through goal setting and annual performance reviews which includes alignment against the Company's standards.	Inspected documentation of procedures for staff performance evaluation and reward. For a sample of employees, determined that annual performance evaluations were conducted.	Exception noted. 1 of 53 employees sampled did not have a performance evaluation during the period.
CC1.5C	On an annual basis, the Senior Director of Compliance, along with General Counsel, requires annual employee training based upon employee location, role, responsibility, and function. The annual training educates employees on federal and state laws and regulations.	For a sample of employees, determined that annual performance evaluations were conducted and that training programs were being monitored and documented in the HR system.	Exceptions noted. 2 of 53 employees sampled did not have documentation of the required annual training. One of the two exceptions is located in a European country and unable to provide documentation. 1 of 53 employees sampled did not have a performance evaluation during the period.
CC2.1	*COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.*		
CC2.1A	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate documentation of required information.	No exceptions noted.
CC2.1B	Architectural diagrams identifying inputs and outputs from the system exist for Nuance healthcare products.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate information on information sources and capture information transformation and processing.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC2.1	*COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (Continued)*		
CC2.1C	Nuance information security policies and procedures are published on the Company Intranet site.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate information on information review and protection.	No exceptions noted.
CC2.2	*COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control necessary to support the functioning of internal control.*		
CC2.2A	Each job role has a specific job description that outlines internal control responsibilities and employees are required to complete the appropriate training. Management monitors training compliance.	For a sample of employees hired or transferred to a new role during the period, obtained the file copy of their job description to determine whether the employees had appropriate background for their job responsibilities. For a sample of employees, verified that the employee participated in required training programs.	Exceptions noted. 2 of 53 employees sampled did not have documentation of the required annual training. One of the two exceptions is located in a European country and unable to provide documentation.
CC2.2B	Quarterly, Information Security and Healthcare Division communicate relevant information to the Chief Technology Officer (CTO). The information is included in the CTO Ops quarterly meetings.	Inspected documentation of the CTO Ops meetings taking place and include communication from the Security and Healthcare Division.	No exceptions noted.
CC2.2C	The Company has contracted with EthicsPoint, a third-party provider, to provide an anonymous mechanism for employees to report improprieties (Whistleblower Hotline).	Inquired of management about the existence of any policy violations and sanctions implemented as a result of the violations. Viewed the posting of the Whistleblower Hotline on the Company Intranet.	No exceptions noted.
CC2.2D	Company-wide announcements are posted to the Nuance Intranet to communicate relevant company information.	Inspected the Company Intranet and determined that it was kept up-to-date and included Company-wide announcements.	No exceptions noted.
CC2.2E	A comprehensive Major Incident Response policy outlines the roles and responsibilities, processes to be followed during various types of major incident events, and how incidents are classified based on severity and type.	Inspected the Major Incident Response policy for definition of roles and responsibilities.	No exceptions noted.
CC2.2F	Nuance Information Security policies and procedures are published on the Company Intranet site.	Inspected the Company Intranet and determined that it included security policies and procedures.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC2.2	*COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control necessary to support the functioning of internal control. (Continued)*		
CC2.2G	System documentation is available to authorized external and internal users that delineates the boundaries of the system and describes the purpose, design, and use of the system. Documentation is available as distributed documents or on the Internet for external user or the Intranet for internal users. Customers are provided with use and support guides that define roles and responsibilities, specify support points of contact, procedures, and processes for obtaining help, reporting issues, and tracking resolution of incidents.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate information on system boundaries, design, purpose, operation and use, and on staff and customer responsibilities. Also inspected application descriptions, product support guides, and application administration documents to confirm adequate descriptions of system capabilities and of staff and customers responsibilities.	No exceptions noted.
CC2.2H	Proposed changes affecting internal staff and/or customers are communicated and confirmed with impacted parties through ongoing communications mechanisms. Changes that result from incidents are communicated to internal and external users through email as part of the implementation and closure process.	Inspected the change process documentation and a sample of weekly changes and associated communications to determine whether system change activities were communicated in a timely manner.	No exceptions noted.
CC2.3	*COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.*		
CC2.3A	The Company has contracted with EthicsPoint, a third-party provider, to provide an anonymous mechanism for employees to report improprieties (Whistleblower Hotline).	Viewed the posting of the Whistleblower Hotline on the Company Intranet.	No exceptions noted.
CC2.3B	The Information Security and Healthcare Division communicates relevant risk assessment results to the Chief Technology Officer (CTO).	Inspected documentation of the CTO Ops meetings taking place and includes communication from the Information Security and Healthcare Division.	No exceptions noted.
CC2.3C	Quarterly CEO, CFO, and Investor relations conducts investor calls to communicate necessary information regarding the Company to external parties.	Verified that quarterly investor calls took place.	No exceptions noted.
CC2.3D	A variety of methods are available for contacting and sharing feedback, including but not limited to Nuance's website, social media channels, and call centers. Nuance representatives are available for direct communication with other stakeholder groups including but not limited to financial analysts, regulators, auditors, and clients.	Inspected various communication mechanisms, including incident communication, change communication, internal Intranet communication, and customer communication.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC2.3	*COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. (Continued)*		
CC2.3E	Formal contracts between Nuance and its third parties define objectives and changes to objectives, including a) roles and responsibilities over security, and b) agreed upon Service Level Agreement (SLA) metrics. Contracts are reviewed by Legal to include the privacy and confidentiality components.	For a sample of contractors, verified that vendor and business partner-signed agreements exist. Inspected information provided to customers and external users regarding confidentiality and privacy.	No exceptions noted.
CC2.3F	System documentation is available to authorized external and internal users that delineates the boundaries of the system and describes the purpose, design, and use of the system.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate information on system boundaries, design, purpose, operation and use, and on staff and customer responsibilities.	No exceptions noted.
CC2.3G	The Company's security responsibilities are outlined in product descriptions, support guides, and administration guides. Detailed application information is available to Company staff on the Intranet.	Inspected documents and Intranet/Internet descriptions of application systems to determine whether they provide adequate information on system boundaries, design, purpose, operation and use, and on staff and customer responsibilities. Verified that detailed application information was available on the Company Intranet.	No exceptions noted.
CC2.3H	Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on customer support websites, in customer guides, and in system documentation. The incident management documents define the incident categorization, escalation, and resolution process.	Inspected application support documents and websites to determine whether they provide sufficient information on reporting issues. Inspected the critical incident handling process documentation.	No exceptions noted.
CC3.1	*COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*		
CC3.1A	The Company has defined risk management policies and processes implemented with the critical security controls (CSA).	Inspected the risk assessment policy and procedure definitions and documentation of the CSA implementation and associated reports, including risk and issue specification.	No exceptions noted.
CC3.1B	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC3.1	*COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (Continued)*		
CC3.1C	Weekly, Nuance Healthcare Leadership meets to discuss all relevant healthcare divisional items including finance, sales, HR, IT, security, operations, development, resourcing, as well as, changes or threats to the business.	Inquired staff and examined evidence of weekly Healthcare Leadership meetings taking place.	No exceptions noted.
CC3.1D	Annually, the Company files a form 10K in accordance with accounting principles.	Verified that 10k is filed annually.	No exceptions noted.
CC3.1E	In response to Section 302 of the Sarbanes-Oxley Act, Nuance has formed a Disclosure Committee which meets at least quarterly to discuss and determine disclosure implications for any recent business developments or changes in the regulatory or policy-making environment. The Disclosure Committee, makes recommendations on specific disclosures for external financial reporting. The drafted quarterly financial statements and the issues documents, are reviewed at the Disclosure Committee meetings.	Inquired staff and examined evidence of quarterly Disclosure Committee meetings taking place.	No exceptions noted.
CC3.1F	Policies and procedures enforced by management are consistent with laws, regulations, and frameworks. Legal reviews and approves changes to policies and procedures.	Inspected policies for legal and regulatory compliance and verified that they are posted on the Company Intranet.	No exceptions noted.
CC3.2	*COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.*		
CC3.2A	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.
CC3.2B	An asset inventory process is in place with a database of application assets.	Inspected asset inventory process and documentation.	No exceptions noted.
CC3.2C	Vulnerability management processes are in place.	Sampled a selection of vulnerability reports and verified that vulnerability scanning process is occurring.	No exceptions noted.
CC3.2D	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC3.3	*COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.*		
CC3.3A	Bi-weekly, the Physical Security and Threat Team meets with Internal Audit to discuss a wide range of internal audit concerns (fraud included). These meetings include discussions on threat of loss of possible assets and when assets may be inappropriately used by employees.	Inquired staff and examined evidence of bi-weekly Physical Security and Threat Team meetings taking place.	No exceptions noted.
CC3.3B	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.
CC3.4	*COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.*		
CC3.4A	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.
CC3.4B	Policies and procedures are in place for assessing and managing system changes, including the assessment of risk.	Inspected the change management process polices and procedures.	No exceptions noted.
CC3.4C	Weekly, Nuance Healthcare Leadership meets to discuss all relevant healthcare divisional items including finance, sales, HR, IT, security, operations, development, resourcing, as well as changes and other threats to the business.	Inquired staff and examined evidence of weekly Healthcare Leadership meetings taking place.	No exceptions noted.
CC4.1	*COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*		
CC4.1A	Policies and procedures are in place defining hiring procedures to ensure staff competence and defining staff roles and responsibilities in formal job descriptions.	Inspected hiring policies and processes regarding required staff competence and policies for security and privacy awareness, training, and compliance. For a sample of employees, inspected personnel files to determine whether the candidate's skills, knowledge, and experience meet the requirements of the position, and whether these qualifications were verified and evaluated as part of the hiring or transfer process.	No exceptions noted.
CC4.1B	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC4.1	*COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (Continued)*		
CC4.1C	A variety of monitoring and evaluation tools and techniques are utilized to assess entity systems, including application, database, network and operating system monitoring, IDS/IPS monitoring, vulnerability scans, penetration testing, and Sumo Logic collection, monitoring, and analysis of log records.	Inspected monitoring documentation. Sampled a selection of vulnerability reports and verified that vulnerability scanning process is occurring.	No exceptions noted.
CC4.1D	Nuance maintains an internal audit function, reporting results of internal audits to the Audit Committee.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the ISRM platform. Inspected documentation of monitoring capabilities and reports. Inspected Sumo log reports.	No exceptions noted.
CC4.2	*COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.*		
CC4.2A	Quarterly, Information Security and Healthcare Division communicate relevant information to the Chief Technology Officer (CTO). The information is included in the CTO Ops quarterly meetings.	Inspected documentation of the CTO Ops meetings taking place and includes communication from the Information Security and Healthcare Division.	No exceptions noted.
CC4.2B	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.
CC5.1	*COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*		
CC5.1A	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.
CC5.1B	Weekly, Nuance Healthcare Leadership meets to discuss all relevant healthcare divisional items including finance, sales, HR, IT, security, operations, development, resourcing, as well as, changes or threats to the business.	Inquired staff and examined evidence of weekly Healthcare Leadership meetings taking place.	No exceptions noted.
CC5.1C	Implementation of the CSA platform includes identification and management of appropriate controls.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC5.2	*COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.*		
CC5.2A	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.
CC5.2B	The Company completes a formal SOX Compliance initiative annually, that serves as its formal risk assessment, process documentation, and control activity testing function over Company internal controls.	Inquired staff and examined documentation of SOX Compliance program.	No exceptions noted.
CC5.2C	Policies are in place governing system acquisition, development, and maintenance.	Inspected policy for system acquisition development and maintenance.	No exceptions noted.
CC5.2D	Monitoring and review capabilities are in place to support technology infrastructure control and management.	Inspected documentation of infrastructure monitoring and management capabilities.	No exceptions noted.
CC5.3	*COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.*		
CC5.3A	Nuance Information Security policies and procedures are published on the Company Intranet site.	Inspected the Company Intranet and determined that it included security policies and procedures.	No exceptions noted.
CC5.3B	Each job role has a specific job description that outlines responsibilities for the role.	Inspected hiring procedures to ensure staff competence and definition of staff authority and responsibility. Inspected policies and procedures defining expected employee actions.	No exceptions noted.
CC5.3C	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.
CC5.3D	Controls are reviewed for a number of certifications or compliance requirements, such as HIPAA, HITRUST, and SOC 2. Reviews are also performed by outside consultants.	Inspected HIPAA, HITRUST, and SOC 2 reports.	No exceptions noted.
CC6.1	*The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.*		
CC6.1A	Inventory of information assets is managed across healthcare products through the tool Terraform. Terraform requires peer review for subsequent changes.	Inspected inventories of information assets and their management. Inspected data classification and retention guidelines.	No exceptions noted.
CC6.1B	Policies and procedures have been established and exist for infrastructure and software hardening that include requirements for implementation of access control software.	Inspected server build specifications for completeness and conformity with security objectives. Inspected access control policies and processes.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC6.1C	Logical access to Company's systems and components is protected through the use of authentication services implemented with native operating system security, native application and resource security, and/or add-on security software.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Inspected a sample of access request tickets to determine whether the request specified the individual, their role and required access, and whether the access was approved by authorized staff. Examined a sample of access termination tickets. Examined application administration guides to verify client user administration capabilities.	No exceptions noted.
CC6.1D	Administrative access to Active Directory, Linux/UNIX, and the Company's servers, databases, storage, and network components is restricted to authorized employees. User activity is logged.	Inspected server build specifications for completeness and conformity with security objectives. Inspected access control policies and processes. Inspected a sample of Active Directory, Linux/UNIX, and infrastructure component access control lists to determine whether access is restricted to appropriate employees based on their defined user role.	No exceptions noted.
CC6.1E	Account sharing is prohibited except for a minimized number of "root" like accesses, in which case mitigating controls are implemented when possible (for example, required use of "su" when accessing a UNIX root account).	Inspected system infrastructure, network, and product descriptions to verify definition of points of access, data flow paths, and use of encrypted communication paths.	No exceptions noted.
CC6.1F	Systems are configured to authenticate users with unique user accounts, passwords, certificates, or licenses and to enforce predefined user account and minimum password requirements 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 terminate after 3 failed login attempts. • The last 10 passwords cannot be reused (5 passwords for privileged accounts).	Inspected the access provisioning, termination, and role-based access control documents to validate controls on access to information systems and components. Inspected a sample of access request tickets to determine whether the request specified the individual, their role, and required access and whether the access was approved by authorized staff. Examined a sample of access termination tickets. Examined application administration guides to verify client user administration capabilities.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC6.1G	Network segmentation has been implemented to isolate the processing environment.	Inspected system infrastructure, network, and product descriptions to verify use of encrypted communication paths. Inspected network diagrams, system infrastructure descriptions, and data center audit reports to determine whether the system includes firewalls and other mechanisms to prevent unauthorized external access and to provide required encrypted customer access.	No exceptions noted.
CC6.1H	Points of access are managed through multi-factor authentication and data mining extensions, each user has a domain to manage access controls. Points of access that flow internally and externally are managed on an as needed basis.	Inspected system infrastructure, network, and product descriptions to verify definition of points of access, data flow paths, and use of encrypted communication paths.	No exceptions noted.
CC6.1I	Encryption is enabled for data at rest.	Inspected system infrastructure, network, and product descriptions to verify use of encrypted communication paths. Inspected policies regarding copying of information to removable media.	No exceptions noted.
CC6.1J	Encryption keys are managed via Key Vault, access to the utility is restricted to authorized individuals.	Inspected policies and procedures regarding key management.	No exceptions noted.
CC6.2	*Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*		
CC6.2A	In order for the Company's employees to obtain system and component access, the employee's manager or supervisor must submit a request ticket which requires management review and approval. The request requires specification of the role and the required accesses. Unique user IDs are assigned to individual users. Access privileges may be assigned by role, by group, or in special cases individually.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Inspected a sample of access request tickets to determine whether the request specified the individual, their role, and required access and whether the access was approved by authorized staff to confirm fulfillment of policy standards.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC6.2B	Access termination is triggered by an email from the human resources system specifying employee termination. A request ticket is created to document and drive implementation of access termination.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Examined a sample of access termination tickets.	No exceptions noted.
CC6.2C	Management performs a periodic review of users and their application privileges to validate that the user privileges are appropriate and limited to authorized personnel, including privilege access.	Inspected user account audit process.	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.*		
CC6.3A	In order for the Company's employees to obtain system and component access, the employee's manager or supervisor must submit a request ticket which requires management review and approval. The request requires specification of the role and the required accesses. Unique user IDs are assigned to individual users. Access privileges may be assigned by role, by group, or in special cases individually.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Inspected a sample of access request tickets and the nature of the access that was established to confirm fulfillment of policy standards.	No exceptions noted.
CC6.3B	Access termination is triggered by an email from the human resources system specifying employee termination. A request ticket is created to document and drive implementation of access termination.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Examined a sample of access termination tickets.	No exceptions noted.
CC6.3C	Management performs a periodic review of users and their application privileges to validate that the user privileges are appropriate and limited to authorized personnel, including privilege access.	Inspected the access provisioning, termination, and role based access control documents to validate controls on access to information systems and components. Examined a sample of access termination tickets.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC6.4	*The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*		
CC6.4A	Physical access controls are in place to restrict access to and within data center facilities. A review of employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary. Employees and contractors are required to return their ID cards during exit interviews, and all ID badges are disabled prior to exit interviews. Therefore employees and contractors must be physically escorted from the Company's facilities at the completion of the exit interview. Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day. The sharing of access badges and tailgating are prohibited by policy.	Inspected policies, audit reports, and other documentation of data center facilities to verify that physical access controls are in place that include the following: -Procedures have been established to restrict physical access to the data centers to authorized employees, vendors, contractors, and visitors. -Security verification and check-in are required for personnel requiring temporary access to the interior data center facility. -Physical access to the data center is reviewed quarterly and verified by the data center operations teams. -Physical access mechanisms (e.g. access card readers, biometric devices, man traps, portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals. -The data center facilities are monitored 24x7 by security personnel.	No exceptions noted.
CC6.4B	Employees and contractors are required to return their ID cards during exit interviews, and all ID badges are disabled prior to exit interviews. Therefore, employees and contractors must be physically escorted from the Company's facilities at the completion of the exit interview. Visitors are required to surrender their badges upon exit.	Inspected a sample of exit interview records to verify that the badges of terminated employees or contractors have been returned and disabled.	No exceptions noted.
CC6.4C	A review of employees and contractors with physical access to sites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary.	Inspected documentation of review of logs of data center physical access.	No exceptions noted.
CC6.5	*The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.*		
CC6.5A	An E-waste procedure exists whereby all equipment identified for disposal is physically destroyed to render the data unreadable.	Inspected data classification and retention guidelines policy and evidence of data and software disposal.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC6.6	*The entity implements logical access security measures to protect against threats from sources outside its system boundaries.*		
CC6.6A	The Company uses firewalls to prevent unauthorized network access. Firewalls and other system mechanisms limit remote access and the types of activities and service requests that can be performed from external connections.	Inspected specification of allowed/disallowed services and open ports.	No exceptions noted.
CC6.6B	Authentication credentials are encrypted during transmission and require multi-factor authentication.	Inspected policies and specification of communication protocols requiring use of encryption.	No exceptions noted.
CC6.6C	Multi-factor authentication is required for customers and engineers accessing the product's application from external sources.	Inspected documentation of application capabilities for customer authentication.	No exceptions noted.
CC6.6D	Boundary protection systems [for example, firewalls, demilitarized zones, Intrusion Detection Systems (IDS), and Intrusion Protection Systems (IPS)] products have been implemented to limit remote access and the types of activities and service requests that can be performed from external connections. Vulnerability scans are run monthly to detect and mitigate weaknesses.	Inspected documentation of network architecture for inclusion of boundary protections, e.g. firewalls and demilitarized zones, network segregation, and for IDS and IPS implementation. Inspected a sample of vulnerability scans to ensure that they are being performed.	No exceptions noted.
CC6.7	*The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.*		
CC6.7A	A data loss prevention (DLP) program is in place to monitor for data loss potential through multiple channels.	Inspected policies and procedures regarding DLP program. Inspected application architectures and infrastructure providing for the secure transmission of information.	No exceptions noted.
CC6.7B	VPN, SSL, and other encryption technologies are used for defined points of connectivity and to protect communications between a processing center and applications/users connecting to a processing center from within or external to customer networks.	Inspected policies and procedures regarding transmission of information. Inspected application architectures and infrastructure providing for the secure transmission of information.	No exceptions noted.
CC6.7C	Nuance maintains an Acceptable Use Policy that is applicable to all employees that access Nuance systems utilizing Nuance-managed devices.	Inspected policy and procedures regarding the use of mobile devices.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC6.8	*The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.*		
CC6.8A	The ability to install software on systems is restricted to change implementation and system administration personnel acting with an approved change request.	Inspected the change management process documentation and the records of its use.	No exceptions noted.
CC6.8B	Multiple times per day, changes to software and configuration parameters are tracked using the SALT tool. Discrepancies are resolved as needed.	Inspected documentation of the use of change detection software.	No exceptions noted.
CC6.8C	As changes are implemented in the environment, secure code reviews are completed prior to implementation.	Inspected documentation of use of secure code reviews.	No exceptions noted.
CC6.8D	Anti-Virus software, Falcon, is installed and in continuous use on servers, workstations, and laptops.	Inspected documentation of the implementation of antivirus/anti-malware software. Inspected reports from regular execution of the antivirus/anti-malware software.	No exceptions noted.
CC7.1	*To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.*		
CC7.1A	Entity standards exist for infrastructure and software implementation and hardening.	Inspected policies for configuration standards and the definitions of such. Inspected server build specifications for completeness and conformity with security objectives.	No exceptions noted.
CC7.1B	Monitoring and logging software, including IDS and IPS software, is continuously active on infrastructure components tracking system performance, resource utilization, and unusual system activity and states. Monitoring software sends alerts to the Site Reliability Center (SRC). An incident may be opened in response to the alerts. Customer support center personnel receive customer telephone, email, or web messages, which may include notification of potential breaches and incidents. Customer support center staff follow defined protocols for recording, resolving, and escalating received reports.	Inspected documentation of the monitoring system and its capabilities. Inspected samples of IDS and IPS records, performance/capacity management records, and SRC monitoring alerts.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC7.1C	Internal and external vulnerability scans are performed weekly by Development Operations to monitor infrastructure and software.	Inspected vulnerability management process documentation. Inspected vulnerability assessments to determine whether they were performed on schedule. Inspected a sample of identified corrective actions resulting from the vulnerability or monitoring processes to determine whether corrective actions were implemented.	No exceptions noted.
CC7.1D	Physical security policies and procedures are in place at all hosting data centers to prevent the introduction of unauthorized components.	Inspected policies and SOC 2 reports from hosting data centers regarding physical security measures.	No exceptions noted.
CC7.2	*The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.*		
CC7.2A	Monitoring and logging software, including IDS and IPS software, native operating system and infrastructure monitors, application monitors, and log aggregation software, is continually active on infrastructure components. These track system performance, resource utilization, user and administrator actions and unusual system activity and states. Monitoring software sends alerts to the Site Reliability Center with monitors continuously. Vulnerability scans are run weekly.	Inspected documentation of monitoring and detection tools to include virus checking and vulnerability scanning software, change detection software, IDS/IPS capabilities, general monitoring capabilities and log aggregation, and analysis software.	No exceptions noted.
CC7.2B	Alerts are sent to the Site Reliability Center for analysis and response. System/application logs are aggregated for analysis at the Security Operations Center. If appropriate, an incident and possibly a change management "ticket" record are created. Operations and security personnel follow defined protocols for resolving and escalating reported events.	Selected a sample of SRC tickets and verified that protocols were being followed.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC7.3	*The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.*		
CC7.3A	The incident management documentation defines the incident categorization, escalation, resolution, and review process. Customers and/or employees may identify issues to support staff who follow defined protocols for documenting, evaluating, and reporting incidents. When a critical incident is identified, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected policies and procedures for the identification and management of security incidents. Inspected policy for the periodic evaluation of their effectiveness.	No exceptions noted.
CC7.3B	The incident management process defines the process for communication and review of security events. Incidents that may affect security compliance or privacy are reported to the secure compliance/privacy officials. The Corporate Privacy Officer and Vice President of Information Security are alerted of the incident and participate as part of the Incident Management Team. Internal and external users are informed of incidents in a timely manner and advised of corrective measures to be taken on their part.	Inspected a sample of documentation of the occurrence of security events, their processing and analysis by the Security Team, communications related to the incidents, and implementation of corresponding corrective actions.	No exceptions noted.
CC7.3C	Bi-weekly, Nuance Security Team conducts a risk and security meeting to address ongoing concerns, relevant changes to the environment, risk assessments, remediation plans, and business success factors.	Inquired staff and examined evidence of bi-weekly Security Team meetings taking place.	No exceptions noted.
CC7.4	*The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.*		
CC7.4A	A comprehensive Major Incident Response policy outlines the roles and responsibilities, processes to be followed during various types of major incident events, and how incidents are classified based on severity and type. Monthly, team meets to review major incidents.	Inspected the incident management process for definition of roles and responsibilities.	No exceptions noted.
CC7.4B	The incident management process and associated security procedures define actions for identification and containment of security incidents.	Inspected procedures for containment and mitigation of security incidents.	No exceptions noted.
CC7.4C	Business Continuity (BC) / Disaster Recovery (DR) plans exist, are implemented at the product level, and periodically tested. The plans address environmental threats resulting from adverse weather, failure of continuity, and recovery procedures in the event of processing anomalies related to security, environmental, and operational incidents.	Inspected procedures for restoration of data and business operations.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC7.4D	Vulnerabilities may be identified through incident analysis or through vulnerability scans which are executed and reviewed weekly. Identified vulnerabilities are assessed, ranked, and remediated as appropriate.	Inspected vulnerability scan reports and a sample of changes driven by the need for vulnerability mitigation.	No exceptions noted.
CC7.4E	Any required remediation activities drive the creation of change requests whose execution is reviewed, authorized, planned and communicated per the change management process.	Inspected a sample of critical incidents and a sample of change management tickets for proper following of protocol and authorization.	No exceptions noted.
CC7.4F	Per the Company's Nuance Healthcare Privacy Policies, there is a process in place that communicates events that resulted in unauthorized use or disclosure of personal information. Event logs are maintained on a Privacy SharePoint site. Incident forms are completed and retained. The Privacy Incident report (completed by Legal) is completed and e-mailed to the customer.	Inspected the policy and observed the existence of a SharePoint site for privacy matters.	No exceptions noted.
CC7.5	*The entity identifies, develops, and implements activities to recover from identified security incidents.*		
CC7.5A	The incident management process and associated operations procedures define actions for restoring data and business operations.	Reviewed past activities, including change requests, for restoration of impacted systems to functional operation.	No exceptions noted.
CC7.5B	The incident handling process defines communication mechanisms and protocols for information related to incident processing. Any required remediation activities drive the creation of change requests whose execution is reviewed, authorized, planned, and communicated per the change management process.	Inspected the incident handling and change management processes. Inspected a sample of change management tickets for proper review, authorization, and documentation of the change request.	No exceptions noted.
CC7.5C	The critical incident management process includes root cause analysis, determination of corrective measures, and implementation schedule. Based on analysis of the issue, change requests are prepared and implemented to address the issues.	Inspected a sample of critical incidents for documentation of root cause analysis and corrective measures.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
CC8.1	*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*		
CC8.1A	Change management policies and procedures exist to govern the process to implement software, infrastructure, and data changes.	Inspected change management process documentation.	No exceptions noted.
CC8.1B	System change requests must be reviewed and approved by the owners of the software and the operational infrastructure, as represented on the Change Advisory Board (CAB), prior to work commencing on and then implementing the requested change.	Inspected a sample of change management tickets for proper review and approval.	No exceptions noted.
CC8.1C	All changes must include specification of acceptance criteria and back-out steps, testing procedures completed to validate the appropriateness of the change, and approval prior to implementation into production. The change process involves the following teams and their discrete responsibilities: • Change Advisory Board (CAB) - approval of change requests • Research & Development - application design and development • Professional Services - creation of initial customer configurations • Quality assurance and test teams - testing • HCHS teams - infrastructure and application deployment	Inspected a sample of change management tickets for proper acceptance, approval, and documentation.	No exceptions noted.
CC8.1D	Changes are developed and tested in separate environments before implementation.	Inspected a sample of change management tickets to ensure implementation plan.	No exceptions noted.
CC8.1E	As part of the change management process, change requests are evaluated to assess the impact of the change on security commitments and requirements.	Inspected a sample of change management tickets for proper approval of implementation plan.	No exceptions noted.
CC8.1F	Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.	Inspected change management process documentation.	No exceptions noted.

SECTION III: CRITERIA, TEST OF OPERATING EFFECTIVENESS AND RESULTS (CONTINUED)

CC#	Criteria	Tests of Operating Effectiveness	Test Results
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. (Continued)*		
CC8.1G	Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Inspected policy regarding test use of sensitive data.	No exceptions noted.
CC9.1	*The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.*		
CC9.1A	Annually, Information Security conducts a risk assessment for Healthcare products summarizing threats and vulnerabilities associated with information and processing integrity of the environment.	Inspected documentation for the implementation of Governance, Risk, and Compliance (GRC) management using the CSA platform.	No exceptions noted.
CC9.1B	Annually, a meeting is held by Legal to renew insurance. Information Security proposes areas of concern where insurance should be bought or renewed which is discussed in the meeting.	Inquired staff and examined evidence of annual Legal meeting reviewing insurance.	No exceptions noted.
CC9.2	*The entity assesses and manages risks associated with vendors and business partners.*		
CC9.2A	The Chief Information Security Officer is responsible for defining and changing confidentiality policies, practices, and commitments. A formal process is used to communicate these to employees, users, related parties, and vendors.	Inquired of the Security Team and reviewed polices and job descriptions.	No exceptions noted.
CC9.2B	Formal contracts between Nuance and its vendors exist. Each contract includes a confidentiality statement in accordance with Company policy, roles, and responsibilities over security, and agreed upon Service Level Agreement (SLA) metrics. Changes to system, services, and SLAs. All contracts are reviewed by Legal.	Inspected policies for contactors. Inspected a sample of Business Associate Agreements (BAAs) and ensured that the agreements contain language on confidentiality and are signed by the contractor.	No exceptions noted.

SECTION III: ADDITIONAL CRITERIA FOR CONFIDENTIALITY

C#	Criteria	Tests of Operating Effectiveness	Test Results
C1.0	**Additional Criteria for Confidentiality**		
C1.1	*The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.*		
C1.1A	Formal contracts between Nuance and its third parties define objectives and changes to objectives, including a) roles and responsibilities over security, and b) agreed upon Service Level Agreement (SLA) metrics. Contracts are reviewed by Legal (privacy) to include the confidentiality statement.	Inspected policies and procedures for data classification, protection, and retention. Inspected Business Associate Agreements (BAAs) for confidentiality requirements.	No exceptions noted.
C1.1B	Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Inspected policies and procedures for data classification, protection, and retention.	No exceptions noted.
C1.1C	Production and non-production design, development, and test environments have the same controls for protection of confidential information.	Inspected application architecture, implementation, and procedures for protecting data confidentiality. Inspected access management processes.	No exceptions noted.
C1.1D	Application, data management, network and operating system security restrict the ability to access, modify, and release data to authorized and authenticated applications and users.	Inspected application architecture, implementation, and procedures for protecting data confidentiality. Inspected access management processes.	No exceptions noted.
C1.1E	Logical access to entity systems and components is protected through the use of authentication services implemented with native operating system security, native application and resource security, and/or add-on security software.	Inspected application architecture, implementation, and procedures for protecting data confidentiality. Inspected access management processes.	No exceptions noted.
C1.1F	Creation and modification of access control rules is managed through the access provisioning and termination process.	Inspected application architecture, implementation, and procedures for protecting data confidentiality. Inspected access management processes.	No exceptions noted.
C1.2	*The entity disposes of confidential information to meet the entity's objectives related to confidentiality.*		
C1.2A	Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	Inspected policies and procedures for data classification, retention, and destruction.	No exceptions noted.

SECTION III: ADDITIONAL CRITERIA FOR AVAILABILITY

A#	Criteria	Tests of Operating Effectiveness	Test Results
A1.0	**Additional Criteria for Availability**		
A1.1	*The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.*		
A1.1A	On a monthly basis, processing utilization and capacity are monitored.	Verified regular collection of performance and utilization data. Inspected records of monthly capacity review meetings.	No exceptions noted.
A1.1B	Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by senior operations and development management.	Inspected records of monthly capacity review meetings and associated forecasts and planning for addressing changes in capacity requirements.	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.*		
A1.2A	Data center management has assessed and provided for environmental threats potentially impacting the systems.	Reviewed SOC 2 Type 2 reports for the data centers to confirm their ability to address environmental threats.	No exceptions noted.
A1.2B	Environment monitoring and detection systems are in place in all data centers to identify anomalies.	Reviewed SOC 2 Type 2 reports for data centers to confirm their ability to monitor and detect environmental issues.	No exceptions noted.
A1.2C	Environmental controls have been implemented to protect systems inside the facilities, including temperature and HVAC controls, fire detection and suppression systems, and power management systems.	Reviewed SOC 2 Type 2 reports to confirm their ability to provide alerts of environmental anomalies.	No exceptions noted.
A1.2D	Critical data has been evaluated and identified and included in appropriate backup and recovery plans. Critical data is replicated multiple times at data centers and is also geo-replicated to the alternate site. Transaction log backups are saved every few minutes with a full backup taken nightly.	Inspected application architecture, implementation, and procedure documents to confirm existence of adequate data backup and restore capabilities.	No exceptions noted.
A1.2E	The Company has contracted for two widely geographically separated facilities which host two active-active instances of the application providing for rapid failover with minimal data loss.	Reviewed application architecture and implementation to confirm ability of the system to failover/failback between the two alternate sites. Reviewed SOC 2 Type 2 reports for the data centers to confirm their ability to address these requirements.	No exceptions noted.

SECTION III: ADDITIONAL CRITERIA FOR AVAILABILITY (CONTINUED)

A#	Criteria	Tests of Operating Effectiveness	Test Results
A1.3	*The entity tests recovery plan procedures supporting system recovery to meet its objectives.*		
A1.3A	Business Continuity (BC) / Disaster Recovery (DR) plans exist, are implemented at the product level, and periodically tested. The plans address environmental threats resulting from adverse weather, failure of continuity and recovery procedures in the event of processing anomalies related to security, environmental, and operational incidents.	Reviewed disaster recovery plans and application recovery procedures and test results.	No exceptions noted.