



Fueling Exceptional Customer Experiences

REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY
TYPE II SOC 2

APRIL 1, 2020 TO MARCH 31, 2021



linford&co llp
cpa firm

Avtex Solutions, LLC

Report on Avtex Solutions, LLC's Description of its Hosting, Contact Center Support, and Managed Services and on its Controls Relevant to Security and Availability

Table of Contents

Description	Page
Section I – Independent Service Auditor's Report	1
Section II – Assertion of Avtex Solutions, LLC's Management	5
Section III – Avtex Solutions, LLC's Description of its Hosting, Contact Center Support, and Managed Services.....	7
Overview of Operations	7
Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security and Availability Criteria.....	10
Security Management.....	10
Personnel Security, Awareness, and Training.....	13
Network Device Security	15
Logical Access	16
Protection from Malicious Software	17
Physical Access	18
Data Transmission.....	19
Monitoring.....	20
Incident Response and Contingency Planning	21
Change Management.....	22
Control Activities	25
Complementary Subservice Organization Controls (CSOC)	26
Avtex's Complementary User Entity Controls (CUEC)	28
Section IV – Independent Service Auditor's Description of Tests of Controls and Results.....	30
Purpose and Objective of the Independent Auditor's Examination	30
Overview of the Internal Control Environment.....	31
Entity-Level Controls	31

Avtex Solutions, LLC

Report on Avtex Solutions, LLC's Description of its Hosting, Contact Center Support, and Managed Services and on Its Controls Relevant to Security and Availability

Table of Contents (continued)

Control Specified by Avtex, Testing Procedures, and Results of Tests	32
Controls Relevant to the Security and Availability Criteria	32
Security Management.....	32
Personnel Security, Awareness, and Training.....	37
Network Device Security	41
Logical Access	44
Protection from Malicious Software	49
Physical Access	51
Data Transmission.....	53
Monitoring.....	54
Incident Response and Contingency Planning	55
Change Management.....	58
Control Activities	60
Section V – SOC 2 Requirements and Controls.....	61
Common Criteria / Security Criteria	62
CC1.0 Common Criteria Related to Control Environment	62
CC2.0 Common Criteria Related to Communication and Information.....	63
CC3.0 Common Criteria Related to Risk Assessment	64
CC4.0 Common Criteria Related to Monitoring Activities.....	64
CC5.0 Common Criteria Related to Control Activities.....	65
CC6.0 Common Criteria Related to Logical and Physical Access Controls.....	66
CC7.0 Common Criteria Related to System Operations	68
CC8.0 Common Criteria Related to Change Management	69
CC9.0 Common Criteria Related to Risk Mitigation	69
Availability Controls	70
Additional Criteria for Availability	70
Section VI – Other Information Provided by Avtex That Is Not Covered by the Service Auditor's Report	71
Management Responses to Section IV Results of Testing.....	71

Section I – Independent Service Auditor’s Report

To the Board of Directors of Avtex Solutions, LLC:

Scope

We have examined Avtex Solutions, LLC’s (Avtex’s) accompanying description of its hosting, contact center support, and managed services system titled, “Avtex Solutions, LLC’s Description of Its Hosting, Contact Center Support, and Managed Services” throughout the period April 1, 2020 to March 31, 2021 (description) based on the criteria for a description of a service organization’s system in Description Criteria section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2020 to March 31, 2021 to provide reasonable assurance that Avtex’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Avtex uses Cologix, vXchnge, Microsoft Azure, and Genesys, subservice organizations, for hosting its production servers, providing backup storage, and for providing cloud-based customer experience and call center technology to support its services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Avtex, to achieve Avtex’s service commitments and system requirements based on the applicable trust services criteria. The description presents Avtex’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Avtex’s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

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

The Information included in section VI, “Other Information Provided by Avtex That Is Not Covered by the Service Auditor’s Report,” is presented by Avtex management to provide additional information and is not a part of the description. The information has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Avtex service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Avtex 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 Avtex's service commitments and system requirements were achieved. Avtex has provided the accompanying assertion titled "Assertion of Avtex's Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Avtex is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (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.

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

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

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section IV of this report titled, "Independent Service Auditor's Description of Tests of Controls and Results."

Opinion

In our opinion, in all material respects:

- a. The description presents Avtex's hosting, contact center support, and managed services that were designed and implemented throughout the period April 1, 2020 to March 31, 2021 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period April 1, 2020 to March 31, 2021 to provide reasonable assurance that Avtex'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 Avtex's controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period April 1, 2020 to March 31, 2021 to provide reasonable assurance that Avtex'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 Avtex's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Avtex, user entities of Avtex's hosting, contact center support, and managed services during some or all of the period April 1, 2020 to March 31, 2021, business partners of Avtex subject to risks arising from interactions with the hosting, contact center support, and managed services,

practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

linford&co llp

April 9, 2021
Denver, Colorado

Section II – Assertion of Avtex Solutions, LLC’s Management

April 9, 2020

We have prepared the accompanying description of Avtex Solutions, LLC (Avtex’s) hosting, contact center support, and managed services titled, “Avtex’s Description of Its Hosting, Contact Center Support, and Managed Services” throughout the period April 1, 2020 to March 31, 2021 (description) based on the criteria for a description of a service organization’s system in Description Criteria section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the hosting, contact center support, and managed services that may be useful when assessing the risks arising from interactions with Avtex’s system, particularly information about system controls that Avtex 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 and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Avtex uses Cologix, vXchnge, Microsoft Azure, and Genesys, subservice organizations, for hosting its production servers, providing backup storage, and for providing cloud-based customer experience and call center technology to support its services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Avtex, to achieve Avtex’s service commitments and system requirements based on the applicable trust services criteria. The description presents Avtex’s controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Avtex’s controls. The description does not disclose the actual controls at the subservice organizations.

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

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

- a) The description presents Avtex’s hosting, contact center support, and managed services that were designed and implemented throughout the period April 1, 2020 to March 31, 2021 in accordance with the description criteria.
- b) The controls stated in the description were suitably designed throughout the period April 1, 2020 to March 31, 2021 to provide reasonable assurance that Avtex’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 Avtex's controls throughout that period.

- c) The controls stated in the description operated effectively throughout the period April 1, 2020 to March 31, 2021 to provide reasonable assurance that Avtex'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 Avtex's controls operated effectively throughout that period.



George Demou
President and Chief Executive Officer

Avtex Confidential. Do Not Redistribute.

Section III – Avtex Solutions, LLC’s Description of its Hosting, Contact Center Support, and Managed Services

Overview of Operations

Overview of the Organization:

Avtex is a full-service Customer Experience (CX) consulting and solution provider focused on helping organizations transform the experiences they deliver to their customers. With an unparalleled breadth of knowledge and experience, and partnerships with leading technology vendors like Microsoft and Genesys, Avtex is uniquely suited to address any CX challenge.

Avtex’s portfolio of solutions and services supports its unique approach to Customer Experience, which includes two key phases, CX Design and CX Orchestration, as follows:

- Avtex’s CX Design solutions and services aid in the process of defining and improving CX. From Journey Mapping to CX Design Thinking, Avtex provides the support clients need to set the foundation for CX success.
- Avtex’s CX Orchestration, solutions and services enable the realization of client CX strategy through people, processes, and technology. From technology implementation to training, Avtex ensures clients have the capabilities to execute their CX strategy.

Avtex Solutions, LLC was founded in 1972 and is based in Bloomington, Minnesota. Avtex was owned by Norwest Equity Partners (NEP), a leading market investment firm based in the Twin Cities, throughout the reporting period.

Services Provided: The company’s contact center solutions include workforce management, speech analytics, quality assurance, predictive dialer, IVR, speech recognition, hosted contact center, predictive behavioral routing, and small business solutions. The business productivity solutions are comprised of portals and collaboration, unified communications, application development, business intelligence, and cloud solutions. In addition, Avtex offers customer experience and marketing solutions, such as marketing automation, CRM, user experience, social enterprise, content management, and mobile solutions. The Contact Center Support Team provides 24/7 support and managed services around the Genesys platforms for both on premise and cloud solutions. They focus on proactive and preventative monitoring and alerting including maintenance, patching, break-fix support, and system design and enhancement.

Principal Service Commitments and System Requirements: Avtex designs its processes and procedures to meet objectives for its hosting, contact center support, and managed services. Those objectives are based on the service commitments that Avtex makes to user entities and the compliance requirements that Avtex has established for their services.

Security commitments to user entities are documented and communicated in their customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the hosting, contact center support, and managed services provided are implemented to grant individuals access to the information they need based on their role while restricting them from accessing information not needed for their role.
- Controlled access to the production infrastructure.
- Data backups.
- Monitoring of system performance metrics and critical application services.

Avtex establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Avtex's system policies and procedures and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how systems are operated, how the internal networks are managed, and how employees are hired and trained.

Components of the System Used to Provide the Services

Infrastructure

Avtex uses subservice organizations to provide its services to its clients in order to achieve operating efficiency and to obtain specific expertise. The following is the principal subservice organization used by Avtex:

- ✓ **Cologix, Inc.**—Cologix hosts Avtex's production IT environment in Minneapolis, Minnesota. Cologix undergoes a Type II SOC 2 examination annually, and the report may be obtained directly from them. Avtex obtains and reviews the SOC 2 report provided by Cologix related to their hosting operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the Cologix SOC report are reviewed and addressed by Avtex.
- ✓ **vXchnge, Inc.**—vXchnge hosts Avtex's production IT environment in St. Louis, Missouri. vXchnge undergoes a Type II SOC 2 examination annually, and the report may be obtained directly from them. Avtex obtains and reviews the SOC 2 report provided by vXchnge related to their hosting operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the vXchnge SOC report are reviewed and addressed by Avtex.
- ✓ **Genesys Telecommunications Laboratories, Inc.**—Genesys provides communication, collaboration, and contact center management support services that Avtex leverages to provide its services. Genesys undergoes a Type II SOC 2 examination annually, and the report may be obtained directly from them. Avtex obtains and reviews the SOC 2 report provided by Genesys related to

their hosting operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the Genesys SOC report are reviewed and addressed by Avtex.

- ✓ **Microsoft Azure**—Avtex uses Azure for backup storage. Azure undergoes a Type II SOC 2 examination annually, and the report may be obtained directly from them. Avtex obtains and reviews the SOC 2 report provided by Azure related to their backup and storage operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the Azure SOC report are reviewed and addressed by Avtex.

People

Avtex has a large staff organized into functional areas so personnel understand their responsibilities within the organization.

Data

Client data is stored within production database instance and file storage. Avtex has implemented security controls to protect the confidentiality of the data. Access controls have been implemented to control access to client data within the Avtex production environment.

Processes and Procedures

Avtex has established and maintains security policies and procedures covering the following areas:

- Antivirus
- Backup
- Change Management
- Data Classification
- Data Privacy
- Data Security and Media Transfer
- Disaster Recovery
- Network Security
- New Hire and On-boarding
- Passwords
- Patch Management
- Risk Management
- Security Incident Management
- Systems Monitoring and Maintenance
- System Hardening
- User Access and Authentication
- Vulnerability Management

Avtex makes these internal policies and procedures, including security policies, available to its personnel on their shared document repository site to provide direction regarding their responsibilities related to the functioning of internal control.

Avtex also provides information to clients and employees on how to report failures, incidents, concerns, or complaints related to the services or systems provided by Avtex in the event there are problems and takes actions as appropriate when issues are raised.

***Relevant Aspects of the Control Environment, Risk Assessment,
Information and Communication, Monitoring, and Control Activities
for the Security and Availability Criteria***

Note: Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction but apply to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting the hosting, contact center support, and managed services.

The security category and applicable trust services criteria were used to evaluate the suitability of design of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them help to determine that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results*.

Security Management

Policies and Procedures: Avtex has defined and documented its security policies and procedures (Company policies and procedures). The Company's policies and procedures address the requirements of the AICPA Trust Services Criteria for Security and Availability (1.1). The areas addressed include:

- ✓ User Access and Authentication
- ✓ Role-based Access
- ✓ Passwords
- ✓ Systems Monitoring and Maintenance
- ✓ System Hardening
- ✓ Antivirus
- ✓ Security Incident Management

- ✓ Risk Management
- ✓ Capacity Planning
- ✓ Data Classification and Data Privacy
- ✓ Physical Security and Access Policy
- ✓ Vulnerability Management
- ✓ Training and Development
- ✓ Network Security
- ✓ Disaster Recovery
- ✓ Security Awareness

Security Program Leadership: The Information Security Officer role has been assigned to the Information Security Officer and the associated responsibilities and accountabilities have been communicated company wide. The Information Security Officer is responsible for the Company's compliance with the requirements of the SOC 2 Security and Availability criteria. The Information Security Officer's responsibilities have been defined in a position description and aligned to the Company policies and procedures relevant to security and availability of client environments (1.2).

The Company makes its information security policies, procedures, and required documentation available to all personnel (1.3). The Company updates its policies, procedures, and required documentation annually, or more frequently, if warranted, in response to environmental or operational changes affecting the security of the systems environment (1.4).

Risk Management Strategy: An organization's risk assessment process is its identification, analysis, and management of risks relevant to the services provided to its clients. It is the responsibility of management to perform these ongoing risk assessments. Key business and operational risks are closely monitored, particularly those related to the quality (e.g., systems monitoring, provisioning) of hosting and managed services, as these are especially critical risks that have the potential to affect the service provided to clients. Avtex also mitigates business risks by adhering to industry-leading practices to reduce risks in all its services.

The Company's policies and procedures for security management address risk assessment, risk management, and incident response. The Company's formal risk analysis addresses the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its clients' application environments (1.5). The security risk analysis includes Avtex personnel input from the different departments at Avtex, including IT, operations, and members of Avtex leadership (1.6). Moreover, Avtex management considers obstacles and threats that may prevent the achievement of meeting business objectives, commitments, and requirements when documenting and rating the risks. Risk mitigation considerations and actions are also documented within the security risk analysis (1.7). The security risk analysis is updated annually, and more frequently when significant changes to the systems occur (1.8).

External Communications: The Company's security and availability commitments are communicated to clients through client agreements (1.9). The agreement specifically outlines the responsibilities as they relate to the confidentiality, access, and security of the Avtex tools and services. In addition to the standard

agreement, Avtex will notify clients in a timely manner documenting any changes or issues that may impact clients' systems, applications, or access; this will include the issue, how it affects the client, why the notification was sent, and a method to contact the support staff.

Avtex has created a client web portal (<https://login.avtex.com>) which allows clients to create and access their support tickets, account site, and collaboration tools. Each client logs into the portal with unique user IDs and passwords and cannot access other clients' applications, tickets, or data (1.10).

Avtex has provided information to clients on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Avtex in the event there are problems. The portal displays the Avtex support number, support emails for support services including managed services, technical assistance, and cloud support, as well as provides an interface to create a support ticket directly from the portal (1.11). Avtex staff are automatically notified when tickets are generated from the portal and they follow-up with the client in a timely manner.

Assessments and Evaluations: Avtex engages a third party to perform an annual external penetration test (1.12). Quarterly, Avtex performs internal vulnerability scans and remediates findings (1.13).

Executive Management: The Avtex leadership team meets on a regular basis to review services provided to clients, business strategy, financial information, effectiveness of operations and internal controls, as well as other items that have a direct relationship to Avtex's operations (1.14). The leadership team plays an important role in the oversight and governance of Avtex, as well as ensuring that Avtex operates within established parameters and complies with ethical and sound business practices.

Management Philosophy and Operating Style: Management understands the importance of oversight and governance. Management believes the best strategy to achieve oversight and governance is to keep leadership highly involved in Avtex's day-to-day operations.

Integrity and Ethical Values: The organizational values and behavioral standards at Avtex are built into the day-to-day activities. Management leads by example and encourages ethical behavior and transparency in all aspects of the business. Avtex expects all employees to conduct themselves honestly and ethically is communicated in the Company's code of conduct (1.15). Avtex's code of conduct and ethics policy provides guidelines and expectations regarding job responsibilities for management and all employees. They are both a statement of business principles and a guide for permissible conduct. All management personnel and each employee must agree to maintain the confidentiality of the information Avtex provides to clients.

Internal Monitoring of Controls: Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has instituted mechanisms to immediately identify and resolve potential problems within the company. Management is responsible for monitoring the quality of the services provided to clients according to requirements specified by each client. All clients have access to a team of service

representatives to communicate and handle client service-related matters. Management's monitoring functions include, but are not limited to:

- ✓ Personnel monitoring the security and availability of the system and services provided to clients.
- ✓ Reviewing activity reports compiled by the system and reviewed by management so that services are delivered in a timely manner.
- ✓ Evaluating and discussing the quality of employee's work products to improve the services provided to clients.

Management performs internal reviews of their control environment to determine that their controls continue to operate effectively (1.16). In this environment, leadership is able to address business issues in a timely manner and consequently reduce risks to the Company and clients. Leadership and employees meet continually to discuss system requirements and progress against outstanding deadlines.

Organizational Structure: A properly defined organizational structure is critical for operating a sound control environment. Avtex's company structure is organized into several departments including Operations, Engineering, Sales, and Marketing, so that client services are handled in the most timely and efficient manner possible. Avtex's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities (1.17). In addition, lines of authority are established throughout Avtex. These lines are communicated through management's operational style, the organizational structure, and employee job descriptions. To increase the operational effectiveness of employees within this structure and so that individuals understand their responsibilities, every position has a job description (1.18).

Personnel Security, Awareness, and Training

Commitment to Competence: Avtex's practices are designed to attract competent personnel in order to provide clients with the highest quality of services. Candidates are carefully identified and interviewed by the management team before being considered for hire. Prospective hires must successfully pass a background investigation before engaging in work-related activities. This process helps Avtex maintain a stable and competent workforce, allowing management to focus on client service. Additionally, employees are strongly encouraged to regularly attend training and attain relevant professional certifications in order to provide an optimum level of service to clients.

Avtex has implemented various methods to communicate information in order to help employees understand and fulfill their roles and responsibilities related to internal control within the organization. These methods include on-board training for new employees, detailed position descriptions, company meetings mediated by members of executive management, other internal meetings, distribution of Avtex's policies and procedures, and communication systems such as voicemail and email. Employees are informed of their responsibility to report operational and control issues to supervisors in the event such issues arise.

New Hire Onboarding Process: Avtex takes great care in the recruitment and selection of individuals that join the Avtex team. Avtex has created an on-boarding process to provide new employees with information,

introductions, and a superior welcome experience. Hiring practices comply with federal, state, and local laws and regulations. To facilitate the onboarding of new employees and contractors, Avtex has created a new hire and onboarding policy (2.1).

Personnel Screening: Avtex promotes a safe and secure working environment for all employees and takes actions to protect employees as well as company property and information. A background check, conducted by the Human Resources (HR) department, is an essential part of the Avtex hiring process. The background check process is used to screen potential employees to determine the safety and security of company property and client information. Avtex requires all new employees and contractors to complete a successful background check (2.2).

Personnel Authorization and/or Supervision: The Company's organizational structure is documented in an organization chart, with lines of authority and supervision (2.3). To help determine that access to systems and Company resources is appropriately granted to new employees, Human Resources completes a new hire checklist for each new hire (2.4).

Onboarding Acknowledgements and Training: The Information Technology (IT) department at Avtex has created information security policies and procedures that help inform employees of their security-related responsibilities. To determine that the policies are understood and agreed to by new hires, an acknowledgement evidencing their understanding and agreement to abide by Avtex policies including the Employee Handbook, Data Privacy Policy, Data Classification Policy, and security policies is required (2.5). In addition, new hires complete security awareness and HIPAA training to help educate employees and contractors on security, data protection, confidentiality, and availability-related risks (2.6).

Employee Portal: The Company maintains an intranet site available to all employees that is used to store policies, procedures, and knowledge related to system administration (2.7).

Personnel Termination: The Company's policies and procedures related to personnel termination emphasize timely removal of employee access and recovery of access control devices upon termination of employment. When employees terminate employment with the Company, HR completes a termination checklist in a timely manner (2.8). The Company maintains the right to discipline or terminate individuals based on a pattern of poor job performance. Under applicable at-will employment law, employees can be terminated at any time for any reason.

Personnel Sanctions: New hires are required to sign a confidentiality agreement, which obligates them to maintain the confidentiality of both Avtex and client data (2.9). New hires and new contractors are also required to sign offer letters or contractor agreements, which communicate that appropriate sanctions, up to and including termination of employment, may be applied against individuals who fail to comply with the Company's policies and procedures (2.10).

Personnel Performance Appraisals: All Avtex's employees are evaluated annually against managerial expectations, general professionalism, technical expectations, areas for growth and improvement, and strengths and contributions (2.11).

Ongoing Personnel Training: Avtex's culture enables employees to explore career paths throughout the company. In addition to the knowledge, skills, and abilities learned to perform current responsibilities, employees are encouraged to seek out leadership in other departments to discuss potential career opportunities and skillsets needed. Avtex has created a training and development policy that outlines employee, management, and Human Resources responsibilities with regard to training (2.12). Annually, Avtex employees and contractors are required to complete security awareness and HIPAA training (2.13). In addition, employees are required to acknowledge Avtex policies including the Code of Conduct, Data Privacy Policy, Data Classification Policy, and security policies annually (2.14). Employees are encouraged to participate in other training and development opportunities as they become available, outlined as follows:

- ✓ Employees are to actively engage in the training process for their current positions, duties, and responsibilities.
- ✓ Employees are encouraged to discuss with their manager areas where they would like to strengthen and develop knowledge, skills, and abilities.
- ✓ Employees are encouraged to work with their manager to create a development plan which enables success in their current position and prepares them for increased responsibilities.
- ✓ Employees are to participate in training opportunities provided by Avtex, including informational lunch and learn sessions about different practices, departments, etc.
- ✓ Employees are encouraged to utilize the tuition reimbursement program for undergraduate or graduate coursework and obtain certification or other training that would be beneficial to the organization as well as the employee's career development.

Employees are encouraged to share knowledge gained from training and development opportunities with the rest of their team to encourage continued learning and innovation among their work areas.

Network Device Security

The systems environment at Avtex is designed to safeguard client environments and data. Network device security controls are important to perimeter security and are described as follows.

Network Security Policy: Avtex maintains a network security policy that covers the network infrastructure such as routers, firewalls, and switches. It defines policies requiring the use of virtual private networks (VPN) and secure protocols for remote access, secure configuration of routers and switches, and the use of access control lists (ACL) on the firewall (3.1). The policy is reviewed on a periodic basis by the Vice President, IT Datacenter Ops, and the Information Security Officer (3.2).

Firewalls, Routers, and Switches: The Company's network is built on multiple layers of firewalls, routers, and switches that are used to manage network traffic. The IT Department maintains network diagrams which document the network architecture (3.3). The firewalls, routers, and switches employ access control lists (ACLs) and rules to block unauthorized public internet access to the internal network, and a Senior Network Engineer reviews these ACLs on a semi-annual basis (3.4). To further determine device security on the Avtex network, Avtex uses a configuration management tool for infrastructure devices that notifies

System Administrators in the event of configuration changes (3.5). Upon notification of configuration changes, System Administrators will evaluate the change is authorized or begin incident response for unauthorized changes.

Network Device Administrator Access: Avtex uses RADIUS for authentication to network devices to include routers, switches, and firewalls (3.6). Network device access requires entry of a valid user ID and password as well as membership within the Network Admins group. The associated permissions and access capabilities, as appropriate, are based upon legitimate business need (3.7).

Remote Network Connections: IT Department personnel may also remotely connect to Avtex's network through a VPN connection that requires authentication using a user ID, password, and multi-factor authentication (3.8). VPNs are configured to transmit data to and from the network securely (3.9).

Logical Access

Information Security Policies and Procedures: Avtex places a high value on the security of its information systems environment. The Company's policies and procedures related to information access management require that access to the Company's systems environment be granted in accordance with business need and restricted to authorized individuals only (4.1).

Account Management: The Company has restricted Administrator-level access privileges (i.e., the ability to add, modify, or delete user access) to appropriate Company personnel who require such access to perform their respective job functions (4.2). Avtex uses two separate Microsoft Windows-based Active Directory (AD) domains as well as a cloud-based IT Systems Management and Remote Monitoring tool called Kaseya. Network access, as well as access to Kaseya, is controlled by the IT Department and is restricted to authorized personnel (4.3). In order to gain access to the systems environment, personnel must first successfully log in to the Company's Microsoft Windows-based AD network or Kaseya using a valid user ID and password (4.4).

Access Establishment, Modification, and Termination: The Company's policies require that a record be maintained documenting access requests, approvals, and actions taken for the establishment, modification, and termination of access to the systems environment. When new employees have their start dates scheduled, Human Resources will send a questionnaire to the IT department to request information such as the type of computer required and what type of access is needed for the new hire's job role. User accounts will be created by the request of the reporting manager or above. Account requests are in the form of a Customer Ticket Number (CTN) and must include formal approval from a manager (4.5). This request will then go to Avtex IT for provisioning. The CTN request will include the start date of the new employee, full name, title, department, phone numbers, manager's name, any special new hardware requests, and any other access requests needed. All CTN access-level requests must be retained for tracking and accounts review/auditing purposes. User access is granted based on the user's job responsibilities as well as business need (4.6). Requests to add new client users to client environments must be approved by an authorized client point of contact, and the user's access level is granted based on the access request (4.7). When employees terminate employment from the Company, and when contractors complete their work

assignments, a system administrator revokes their access in a timely manner (4.8). When Avtex receives requests to terminate the access of client employees to Kaseya, access is disabled within 24 hours (4.9).

Complementary User Entity Controls: *User entities are responsible for notifying Avtex in the event that access for their employees needs to be modified or removed.*

Password Management: The Company has established and implemented policies and procedures for password management. Passwords are established according to a standard, which requires that: a) all user IDs must have a password; b) passwords are user-created and at least eight characters in length; c) passwords must be complex, meaning they must contain upper- and lower-case alphabetic, numeric, and special characters; d) the previous twelve passwords cannot be used; and e) passwords of individuals must be changed at least every 90 days (4.10). A password policy has been created that requires the standards previously mentioned to be implemented. Shared user accounts are also prohibited.

Periodic User Access Reviews: Annual entitlement reviews of administrator access within the Avtex environment are performed and access is modified based on the results of the reviews as needed (4.11).

Client Access Segregation: Avtex clients have their own logically segregated environments that are used by client applications. As a result, Avtex clients have access to only their own data and do not have access to any other client's data (4.12).

Laptop Encryption: Avtex has taken steps to reduce the risk associated with a laptop being lost or stolen. Avtex encrypts the hard drives of all employee laptops (4.13).

Complementary User Entity Controls: *User entities are responsible for encrypting data in their environment for which Avtex provides managed services.*

Hardware and Data Disposal: Avtex's policies related to media protection address the handling of devices and media that may potentially contain sensitive Company or client data, including PII and ePHI (4.14). Avtex defines specific requirements for hardware and data disposal in its security policies (4.15). All electronic equipment is wiped of all data or is physically destroyed by a well-known third party who specializes in secure media destruction (4.16).

Session Lock: Employee workstations are configured to enable a screensaver after a modest period of inactivity, and a password is required to regain access to the workstation (4.17).

Protection from Malicious Software

Acceptable Use of Software, Hardware, and the Internet: Avtex obtains employee acknowledgement of the employee handbook which contains language regarding the acceptable use of software, hardware, and the internet on Avtex's systems. Acceptable use language within the employee handbook prohibits the download or importation of programs, files, or documents into the Company's systems environment except as authorized by Avtex (5.1). All computers, including desktops, laptops, and handheld devices provided

by Avtex, are to be used for company business purposes and in a manner that poses no risk to the Company or the Company's clients. Employees who receive email containing a virus or who detect a virus on company-provided equipment must immediately notify appropriate technical support personnel.

Workstation and Server Hardening: Avtex's network nodes are provisioned and hardened in a manner which helps support the confidentiality, integrity, and availability of data and systems. Improper provisioning and hardening of the nodes may result in network exploitation by external or internal threats. Avtex has developed a system hardening policy that outlines the requirements for hardening servers and workstations. The policy requires that all images deployed on servers and workstations are up-to-date on security patches (5.2).

Antivirus Software: One of Avtex's goals is to provide a computing network that is virus free. To help achieve that goal, Avtex has created an antivirus policy which requires that Avtex deploy antivirus software on its workstations and servers which may access or support clients' system environments (5.3). Avtex has configured the antivirus software to update the antivirus signature definitions automatically and perform regularly scheduled scans on all employee workstations and hosted servers (5.4).

Security Patch Management: Avtex manages the application of software patches, including critical security patches, to Windows-based system components in client systems' environments at the request of the source code vendor. Avtex patches internal workstations, managed services servers, and internal servers as needed (5.5). By default, Avtex uses system rules and configurations to automatically patch servers. When implementing Avtex services, user entities may request servers be manually patched or not patched at all. For managed servers, Avtex audits all patches and patching details monthly and updates the server and patching details as needed (5.6).

Complementary User Entity Controls: User entities who requested Avtex to not patch servers are responsible for managing server security patches.

Intrusion Detection: Avtex has implemented an intrusion prevention system that monitors network activity and blocks IP addresses as needed. A third-party vendor monitors the network for unauthorized access attempts and notifies Avtex of any issues. Avtex follows up on potential issues as needed and takes corrective action to prevent unauthorized access (5.7).

Physical Access

In April 2020, due to the COVID-19 pandemic, Avtex employees transitioned to a remote workforce.

Building Security: Avtex is located in Bloomington, Minnesota in a multi-tenant building. All personnel are issued a single card key to access the building and office. The building is unlocked from 6:00 am to 7:00 pm, Monday through Friday, 7:00 am to 3:00 pm on Saturday, and at all other times, the building is locked, and a card key is required to enter (6.1).

Office Suite Security: Avtex's office suite has one main entrance with a receptionist, which is physically secured by a card key system and access is provided only to authorized personnel (6.2). All other entrances require a key card, but do not have a receptionist. The Office Administrator maintains a record of the card key issued to each new hire. All visitors are received by an authorized employee who must monitor the visitor while they are in the office (6.3).

Server Room: There is one additional area which is card key access controlled—the server room. The server room contains certain network devices and servers that support file systems and domain authentication. Physical access to the server room is restricted to authorized IT Department and management personnel (6.4).

Physical Access Administration: The card key system is managed by the Office Administrator based upon authorization from the HR Coordinator. New hires are provided a card key that enables them to access the office suite. Management approves any non-standard access (e.g., server room access, etc.). When personnel terminate employment from Avtex, their card key is collected on the individual's last day of work and is disabled in the card key system (6.5). The card key system maintains a log of card key activity. The logs are used to investigate suspicious activity on an as-needed basis.

Colocation and Managed Services Provider: Avtex's systems environment, which supports its clients' applications, is hosted by either Cologix or vXchnge. Only authorized management and IT Department personnel may contact Cologix or vXchnge on behalf of Avtex and request services (6.6). Avtex also restricts physical access to the Avtex cabinets within the Cologix and vXchnge data centers to authorized employees only (6.7).

Data Transmission

Avtex uses three primary methods to securely transfer data between clients and remote employees to internal Avtex systems. They include the following:

- ✓ **Secure File Transfer Protocol (SFTP):** Avtex allows for larger, confidential files to be transmitted via Secure File Transfer Protocol (SFTP). SFTP data connections between Avtex and clients use industry-standard, strong encryption algorithms (7.1).
- ✓ **Kaseya Security:** Kaseya incorporates the use of AES 256-bit encryption to encrypt data submitted by Avtex clients through Kaseya (7.2). Kaseya provides a certificate to authenticate to the end user that the server they are communicating with is the server they believe it to be.
- ✓ **VPN Connectivity:** For authorized Avtex employees and authorized clients, Avtex provides secure Virtual Private Network (VPN) access (7.3). VPN connections from the Avtex network to clients and employees are encrypted. Users are authenticated against the Avtex firewall and must have a valid username, password, and multi-factor authentication configured within the firewall to access Avtex's network.

Client Data Segregation: For the SFTP services mentioned previously, each Avtex client has their own directory in which to put client data. Avtex restricts access to each client home directory to only a single authorized client user and locks the user to only that home directory (7.4).

Complementary User Entity Controls: User entities are responsible for ensuring transmissions between themselves and the Avtex network are encrypted to the level required for their organization and notifying Avtex when issues with the connections arise.

Monitoring

Avtex employs multiple software tools and supporting processes to manage and monitor its technical environment which consists of hosted and managed services for their clients and internal Avtex infrastructure. Through the use of these multiple tool suites, Avtex employees are able to quickly identify and document failures, incidents, or other anomalies and start the remediation process in a timely manner. Each tool suite and supporting process is assigned a senior Avtex employee as the monitoring owner.

Avtex's policies related to logging and monitoring of information systems activity and health require the collection and review of information systems activity in audit logs, access reports, and security incident tracking reports (8.1).

System Monitoring and Logging: Avtex monitors and logs information system activity for their clients' environments as well as the core infrastructure shared among clients (8.2).

Complementary User Entity Controls: User entities are responsible for maintaining audit logs within their environments.

Monitoring and Follow-up: Avtex Managed Services (MS) and IT Operations personnel receive alerts, primarily via email, from the multiple monitoring tools deployed throughout the Avtex corporate and managed infrastructure. They subsequently manually enter these events into the Avtex ticket management system. Tickets can be entered into the ticket management system 24/7. Avtex's MS and IT Operations personnel review the IT infrastructure logged events in real time and alert on specific events and issues related to key IT infrastructure components (8.3). Issues that require additional follow-up are entered into the ticketing system, appropriately acted upon, and monitored to resolution (8.4).

Subservice Organizations: Avtex uses industry-recognized subservice organizations to achieve operating efficiency and to obtain specific expertise. The following are the principal subservice organizations used by Avtex in support of its Services:

- ***Cologix, Inc.***—The Avtex information technology (IT) environment includes Cologix colocation facility located in Minneapolis, Minnesota. Housed within the colocation facilities are server cabinets supporting Avtex's operating system platforms, networking components (routers,

switches, firewalls, and load balancers), and data storage devices. Avtex's IT personnel that support these components are based at the corporate office facilities in Bloomington, Minnesota.

- **vXchnge, Inc.**—The Avtex information technology (IT) environment includes vXchnge colocation facility located in St. Louis, Missouri. Housed within the colocation facilities are server cabinets supporting Avtex's operating system platforms, networking components (routers, switches, firewalls, and load balancers), and data storage devices. Avtex's IT personnel that support these components are based at the corporate office facilities in Bloomington, Minnesota.
- **Genesys Telecommunications Laboratories, Inc.'s PureCloud**—PureCloud is a suite of cloud services for enterprise-grade communications, collaboration, and contact center management. PureCloud is used by Avtex as well as resold to Avtex customers. Avtex provides its customers technical and integration support for PureCloud.

Avtex obtains and reviews the SOC 2 report provided by Cologix, vXchnge, Microsoft Azure, and Genesys to determine whether controls are designed and operating effectively **(8.5)**. Additionally, applicable complementary user entity controls in the SOC 2 reports are reviewed and addressed by Avtex.

Incident Response and Contingency Planning

Avtex provides support around its two strategic partners—Microsoft and Genesys. Avtex has two support teams that work together to provide seamless support across those partners' technologies.

The Managed Services (MS) team provides 24/7/365 managed services around Microsoft-based technologies and services. The MS team focuses on supporting client's infrastructure by monitoring, patching, and providing full-service management of those technologies. The MS team also provides comprehensive application support for Business Productivity (Office 365), Dynamics365, and Unified Communications (Skype for Business and Teams).

The Contact Center Support (CCS) team provides 24/7 support and managed services around the Genesys platforms for both Premise and Cloud solutions. The CCS team focuses on proactive and preventative monitoring, alerting, patching, break-fix support, maintenance, and system design and enhancement. Additionally, the CCS team is staffed over the weekends for full 24/7/365 emergency support for the PureCloud product.

Incident Response Plan: Avtex defines an incident as, "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Avtex has established and implemented a Security Incident Management Policy and Security Incident Management Procedures to be activated in the event a security or availability incident occurs **(9.1)**. The Security Incident Management Policy and Security Incident Management Procedures have been communicated to appropriate personnel. The Security Incident Management Policy and Procedures address preparation, notification, incident identification and tracking, classification and prioritization, containment, eradication, reporting, root cause analysis, and lessons learned. The Security Incident Management Policy and

Procedures are reviewed and updated annually and more frequently based upon incident outcomes and lessons learned, as appropriate (9.2).

Incident Monitoring and Recordkeeping: Avtex maintains a record of all security and availability incidents within their ticketing system. Of the low, medium, high/emergency ticket prioritization categories, security and availability incidents are categorized as high/emergency (9.3). The incident records include, as appropriate and applicable, the following: a) description of the incident and relevant facts and assumptions; b) root cause analysis; and c) outcomes. Incidents and problems logged on behalf of clients are documented, addressed, and resolved in a timely manner (9.4). Avtex's policy is to issue a Critical Incident Report (CIR) within 24 business hours. If the CIR is not closed within 24 hours, the CIR is still issued with the latest status of the incident.

Offsite Recovery Location: Avtex maintains a backup copy of its essential production systems, including client data, at an offsite location (9.5). The offsite location is at a sufficient distance to provide safeguards against localized disasters (e.g., tornados).

Backup Data Encryption: Backup data is stored in Azure. Backup data is encrypted at rest (9.6).

Testing Procedure: The Avtex Disaster Recovery Policy identifies the requirement to test the disaster recovery plan including tabletop exercises and restoration of data from backups. Disaster recovery scenarios are tested in any year that a disaster was not declared (9.7).

Notification in the Case of Breach: Avtex's policies and procedures related to breach notification, and incident response plan, are consistent with the HIPAA Breach Notification Rule. In the event of a breach, Avtex is required to notify each client affected by the breach in a timely manner and in conformity with the contractual obligations in place (9.8). Avtex tailors its breach notification process to each client in accordance with the parameters within each business associate agreement (BAA). Avtex's business associate agreement with subservice organizations and contractors obligates such organizations to report breaches, if any, to Avtex in a timely manner (9.9).

Complementary User Entity Controls: User entities are responsible for responding to incidents occurring in their environment.

Complementary User Entity Controls: User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.

Change Management

Avtex defines change management as the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the Avtex IT Infrastructure. The change management process begins with the creation of a change request and ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

Requests for changes (RFC) made to Avtex's information systems require evaluation and authorization prior to implementation to maintain system stability and reliable operation. Changes may be requested by internal Avtex employees, external customers, clients, and other third-party vendors. It is crucial that changes are implemented according to a consistent approach to minimize service disruption. To facilitate a structured change management process, Avtex has documented procedures which outline the requirements and appropriate protocols for enacting changes to key/critical information systems **(10.1)**.

Formal Change Request: The change process begins when a requestor initiates a change request and documents what change is desired from a functional perspective. The requestor is also responsible for reviewing results of the change and acknowledging the closure of the change. Changes may be requested by anyone in the company. A change request is submitted via an electronic change request form on the company intranet. **(10.2)**.

Classifying the Category of a Change

Category	Category Definition
Emergency	Emergency changes are defined as changes that need to be evaluated, assessed and either rejected or approved in a short space of time. Simply defining a change as an emergency does not automatically require that the change be implemented. The Emergency Change Advisory Board (ECAB) will assess Emergency changes, approve, or deny the change, and notify the change requestor.
Normal	A normal change refers to changes that must follow the complete change management process. Normal changes are often categorized according to risk and impact to the organization. A normal change will proceed through all steps of the change management process and will be reviewed by the Change Advisory Board (CAB).
Standard	A standard change is a low-risk change to a service or infrastructure that is pre-authorized by the CAB and that has an accepted, established, and well documented procedure. A library of Standard Changes will be maintained, and Standard Changes will be reviewed at least annually.

Authorizing Standard Changes: All Standard changes must go before the CAB to receive pre-approval. A Standard change is a change to the infrastructure that follows an established path, is documented, and is the approved solution to a specific requirement or set of requirements. Examples include password changes, updates to certain document templates, and routine systems patching or maintenance. The elements of a Standard change are:

- ✓ The tasks in a Standard change are low risk, documented, well-known, and proven.
- ✓ A Standard change has been reviewed and pre-approved by the CAB.
- ✓ The library of Standard changes is periodically reviewed by the CAB.

Authorizing Normal Changes: All Normal changes must go before the CAB for approval. Because of the impact of such changes on the IT environment or the number of users who will be affected, these changes cannot be authorized by a single individual. The individual might not understand the full impact of the change or might not understand the impact from the point of view of a particular function within the organization. For example, the individual might not understand the implications of a change in security, capacity, or service level. The CAB, on the other hand, has a broad membership with enough cumulative knowledge to fully understand the implications of the change.

Authorizing Emergency Changes: All Emergency changes must go before the Emergency CAB for approval. The emergency change process enables an organization to continue normal operations or restore them as quickly as possible and follows the normal change process at an accelerated rate. Emergency changes need to be implemented quickly—for example, to prevent a potential security breach or fix a business-critical application outage. Because emergency changes are generally more disruptive and often prone to failure, the number of proposed emergency changes should be kept to an absolute minimum. Time constraints allow only limited testing and require that normal processes and controls be bypassed. Emergency changes cannot be authorized by a single individual and must be reviewed and approved by at least three members of the ECAB. An Emergency change request will automatically trigger an email notification to the ECAB and appropriate management for review.

The Emergency CAB (ECAB) membership includes the VP of IT, the IT Operations Manager and the Information Security Officer.

Change Advisory Board: The CAB is responsible for evaluating the merit of change requests and determining the classification and impact of requested changes. Changes marked as “awaiting implementation” are reviewed and approved by the CAB. The CAB meets weekly to review and approve change requests except during change freeze periods (10.3).

Change Manager: The change manager is responsible for scheduling and implementing the change. The change manager is required to document the completion of the change in the change tracking system.

Decision-making Responsibility Matrix

Standard Change	Normal	Emergency Change
Preauthorized by CAB	CAB	Emergency CAB

Changes must be authorized in accordance with the decision-making responsibility matrix prior to implementation in production (10.4).

Change Testing: Test plans and test data should be developed, used, and reviewed by the appropriate parties to validate the design and effectiveness of the changes are meeting system commitments and requirements prior to implementation. Deviations to the planned results must be analyzed and may need to be submitted to a developer for review. Depending on the nature of the change, user acceptance testing may be required

to validate the change prior to implementation. Test activities are documented in the request for change ticket **(10.5)**. If testing is not required, it is noted in the request for change ticket.

Security Program Integration with Change Management Processes: The Change Management process includes steps to consider the potential security implications of significant changes to the IT environment. For changes that impact Avtex's commitments and requirements relevant to security and availability, Avtex communicates the potential security and availability impact to those users in a timely manner **(10.6)**.

Complementary User Entity Controls: User entities are responsible for notifying Avtex of the requirements of their client change management processes so that Avtex follows the appropriate controls to mitigate the risk of changes to client environments.

Control Activities

Control activities are the specific functions performed by Avtex management and employees to address the individual risks associated with the achievement of the company's objectives. Properly functioning control activities support company operations and can be objectively viewed and independently tested. Control activities can take the form of automated and/or manual controls and function in a combination of systems and business processes.

Avtex has established and implemented policies and procedures to determine that periodic assessments and evaluations are performed that consider the elements of security and availability as it applies to AICPA trust services criteria. Findings, recommended actions, and the Company's remediation decisions are communicated to appropriate personnel. The Company engages a third-party auditor to perform a SOC 2 audit annually. Additionally, Avtex has developed a set of policies that establish expected behavior with regard to the Company's control environment **(11.1)**. Avtex management also segregates responsibilities and duties across the organization and within the infrastructure environment to mitigate risks to the services provided to its clients **(11.2)**.

Other control activities relevant to the security and availability criteria are specified throughout Sections III and IV of this report.

Complementary Subservice Organization Controls (CSOC)

Avtex's controls related to the hosting, contact center support, and managed services cover only a portion of the overall internal control for each user entity of Avtex. It is not feasible for the control objectives related to the hosting, contact center support, and managed services to be achieved solely by Avtex. Therefore, each user entity's internal controls must be evaluated in conjunction with Avtex's controls, and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization, described as follows:

	vXchnge Complementary Subservice Organization Controls	Related Control Criteria
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-6.5
2.	The subservice organization is responsible for managing and resolving security and availability incidents related to the data center facility in a timely manner.	CC7.2-7.5
3.	The subservice organization is responsible for ensuring the hosted environments are available 24/7/365.	CC7.1-CC7.2
4.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.1-CC7.2

	Cologix Complementary Subservice Organization Controls	Related Control Criteria
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-6.5
2.	The subservice organization is responsible for managing and resolving security and availability incidents related to the data center facility in a timely manner.	CC7.2-7.5
3.	The subservice organization is responsible for ensuring the hosted environments are available 24/7/365.	CC7.1-CC7.2
4.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.1-CC7.2

	Azure Complementary Subservice Organization Controls	Related Control Criteria
1.	The subservice organization is responsible for providing the physical security controls protecting the backup storage from unauthorized access.	CC6.4-6.5
2.	The subservice organization is responsible for managing and resolving security and availability incidents related to the data center facility in a timely manner.	CC7.2-7.5
3.	The subservice organization is responsible for ensuring the hosted environments are available 24/7/365.	CC7.1-CC7.2
4.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.1-CC7.2

	Genesys Complementary Subservice Organization Controls	Related Control Criteria
1.	The subservice organization is responsible for providing the physical security controls protecting the PureCloud servers from unauthorized access.	CC6.4-6.5
2.	The subservice organization is responsible for managing and resolving security and availability incidents related to the PureCloud platform in a timely manner.	CC7.2-7.5
3.	The subservice organization is responsible for ensuring the PureCloud platform environment is available 24/7/365.	CC7.1-CC7.2
4.	The subservice organization is responsible for providing the environmental controls protecting the PureCloud platform.	CC7.1-CC7.2

Avtex's Complementary User Entity Controls (CUEC)

The hosting, contact center support, and managed services provided by Avtex for user entities and the controls at Avtex cover only a portion of the user entity's overall system of internal control. It is not feasible for the controls related to the hosting, contact center support, and managed services to be achieved solely by Avtex. Therefore, each user entity's internal control must be evaluated in conjunction with Avtex's controls, and the related tests and results described in Section IV – Independent Service Auditor's Description of Tests of Controls and Results of this report, taking into account the related complementary user entity controls identified under each area, where applicable.

This section highlights additional control activities that Avtex believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. This list is not intended to be, and is not a complete listing of, the controls that provide a basis for the achievement of the security control criteria.

	Complementary User Entity Controls	Related Control Criteria
1.	User entities are responsible for notifying Avtex in the event that access for their employees needs to be modified or removed.	CC6.3
2.	User entities are responsible for encrypting data in their environment for which Avtex provides managed services.	CC6.1, CC6.7
3.	User entities who requested Avtex to not patch servers are responsible for managing server security patches.	CC6.8
4..	User entities are responsible for ensuring transmissions between themselves and the Avtex network are encrypted to the level required for their organization and notifying Avtex when issues with the connections arise.	CC6.7
5.	User entities are responsible for maintaining audit logs within their environments.	CC7.1, CC7.2
6.	User entities are responsible for responding to incidents occurring in their environment.	CC7.3, CC7.4, CC7.5
7.	User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.	CC7.4

8.	User entities are responsible for notifying Avtex of the requirements of their client change management processes so that Avtex follows the appropriate controls to mitigate the risk of changes to client environments.	CC8.1
----	--	-------

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation and tests of operating effectiveness is intended to provide users of the report with information sufficient to obtain an understanding of those aspects of Avtex's controls that may be relevant to clients' internal controls. This report, when coupled with an understanding of the internal controls in place at each client, is intended to assist in the assessment of the total internal control surrounding the hosting and managed services provided by Avtex.

Our examination was limited to those controls performed in Avtex's Bloomington, Minnesota, office in support of the hosting, contact center support, and managed services. It is each stakeholder's responsibility to evaluate this information in relation to the internal controls in place at each client to obtain an overall understanding of the internal controls and assess control risk. The controls provided by each client and Avtex must be evaluated together. If effective control activities are not in place at the client, Avtex's controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls surrounding Avtex's hosting and managed services. Our tests of controls were performed throughout the period of April 1, 2020 to March 31, 2021 and were applied to those controls relating to the applicable trust services criteria.

The description of controls is the responsibility of Avtex's management. Our responsibility is to express an opinion that the controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control criteria, specified by the AICPA, were achieved during the period covered by our report.

Any exceptions noted by Linford & Company LLP regarding the operating effectiveness of the controls identified related to the applicable control criteria or the level of compliance with the controls are presented in this section under the caption, "Results of Testing." Concerns identified herein are not necessarily weaknesses in the total system of internal control at Avtex, as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of Avtex to attain the stated criteria are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-Level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination of the tests of operating effectiveness was for the period of April 1, 2020 to March 31, 2021 and was applied to those controls relating to the applicable trust services criteria specified by the AICPA.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of Avtex's control environment, including Avtex's organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* Avtex's organizational structure, including the segregation of functional responsibilities, personnel policies, and other policies and procedures.
- ✓ *Inquired* through discussion with management personnel responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* personnel in the performance of their assigned duties.

No exceptions were noted in entity-level testing.

* * * * *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the operating effectiveness of controls.

Control Specified by Avtex, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. Avtex Management specified the control activities, and the AICPA specified the related control criteria in Section V – SOC 2 Requirements and Controls.

Controls Relevant to the Security and Availability Criteria

Security Management

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
1.1	The Company's policies and procedures address the requirements of the AICPA Trust Services Criteria for Security and Availability.	<i>Inspected</i> the Company's policies and procedures relevant to the requirements of HIPAA and the Security and Availability criteria, and noted that the Company's policies and procedures addressed the requirements.	No exceptions noted.
1.2	The Information Security Officer's responsibilities have been defined in a position description and aligned to the Company policies and procedures relevant to security and availability of client environments.	<i>Inspected</i> the Information Security Officer position description and noted that security and availability-related responsibilities were defined. <i>Inspected</i> the Avtex organizational chart and noted that the Information Security Officer role was assigned.	No exceptions noted. No exceptions noted.

Security Management (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
1.3	The Company makes its information security policies, procedures, and required documentation available to all personnel.	<i>Inspected</i> the corporate intranet and noted that policies and procedures were available to Avtex employees.	No exceptions noted.
1.4	The Company updates its policies, procedures, and required documentation annually, or more frequently, if warranted, in response to environmental or operational changes affecting the security of the systems environment.	<i>Inspected</i> the Company policies and procedures and noted that the documents were updated recently.	No exceptions noted.
1.5	The Company's formal risk analysis addresses the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its clients' application environments.	<i>Inspected</i> the risk management policy and noted that it addressed the elements of the risk management process including risk identification, analysis, and response. <i>Inspected</i> the risk analysis and noted that it addressed the security and availability risks to its clients' environments.	No exceptions noted. No exceptions noted.
1.6	The security risk analysis includes Avtex personnel input from the different departments at Avtex, including IT, operations, and members of Avtex leadership.	Noted through inspection of the risk matrix, that personnel from across Avtex provided input into the risk assessment process.	No exceptions noted.

Security Management (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
1.7	Risk mitigation considerations and actions are also documented within the security risk analysis.	<i>Inspected</i> the security risk analysis documentation and noted that risk mitigation considerations and actions were documented.	No exceptions noted.
1.8	The security risk analysis is updated annually, and more frequently when significant changes to the systems occur.	<i>Inspected</i> the security risk analysis and noted that it was updated recently and included risks to the Avtex IT environment and the potential impact and likelihood of the risks occurring.	No exceptions noted.
1.9	The Company's security and availability commitments are communicated to clients through client agreements.	<i>Inspected</i> the standard customer agreement template and noted that Avtex communicated its security and availability commitments to customers.	No exceptions noted.
1.10	Each client logs into the portal with unique user IDs and passwords and cannot access other clients' applications, tickets, or data.	<i>Inspected</i> the Avtex portal login and determined that it was configured to require a unique user ID and password and that other client data could not be accessed.	No exceptions noted.
1.11	The portal displays the Avtex support number, support emails for support services including managed services, technical assistance, and cloud support, as well as provides an interface to create a support ticket directly from the portal.	<i>Inspected</i> that the portal and noted it displayed the help desk number as well as a link to open a help desk ticket in the event that there was an error, or the customer had any questions.	No exceptions noted.

Security Management (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
1.12	Avtex engages a third party to perform an annual external penetration test.	<i>Inspected</i> the third-party penetration test report and noted it was completed.	No exceptions noted.
1.13	Quarterly, Avtex performs internal vulnerability scans and remediates findings.	<i>Inspected</i> the vulnerability scanning tool and accompanying documentation and noted an internal scan was performed for a sample of quarters and vulnerabilities were reviewed for remediation.	No exceptions noted.
1.14	The Avtex leadership team meets on a regular basis to review services provided to clients, business strategy, financial information, effectiveness of operations and internal controls, as well as other items that have a direct relationship to Avtex's operations.	<i>Inspected</i> meeting minutes and noted the leadership team met regularly to discuss matters impacting Avtex's operations.	No exceptions noted.
1.15	Avtex expectations for all employees to conduct themselves honestly and ethically is communicated in the Company's code of conduct.	<p><i>Inspected</i> the company's code of conduct and the ethics policy and noted that the documents explicitly stated the expectations for employees to conduct themselves honestly and ethically in all circumstances.</p> <p><i>Observed</i> management and employees during fieldwork and noted that management and employees conducted themselves with integrity.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Security Management (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
1.16	Management performs internal reviews of their control environment to determine that their controls continue to operate effectively.	<i>Inspected</i> internal audit task boards and documentation and ascertained that management took steps to monitor the control environment to determine that controls were operating effectively.	No exceptions noted.
1.17	Avtex's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	<i>Inspected</i> Avtex's organizational chart and noted that the chart defined the organizational structure organized into several departments to facilitate information flow and establish responsibilities.	No exceptions noted.
1.18	To increase the operational effectiveness of employees within this structure and so that individuals understand their responsibilities, every position has a job description.	For a sample of unique job positions, <i>inspected</i> the job description for the position and noted the job description correlated with the job function.	No exceptions noted.

Personnel Security, Awareness, and Training

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
2.1	To facilitate the onboarding of new employees and contractors, Avtex has created a new hire and onboarding policy.	<i>Inspected</i> the new hire and onboarding policy and noted that it documented onboarding requirements for new hires.	No exceptions noted.
2.2	Avtex requires all new employees and contractors to complete a successful background check.	For a sample of new hires during the examination period, <i>inspected</i> background check results and ascertained that a background check was completed as a condition of employment for each new hire in the sample.	No exceptions noted.
2.3	The Company's organizational structure is documented in an organization chart, with lines of authority and supervision.	<i>Inspected</i> the organization chart and noted that it addressed lines of organizational authority and supervision.	No exceptions noted.
2.4	To help determine that access to systems and Company resources is appropriately granted to new employees, Human Resources completes a new hire checklist for each new hire.	For a sample of new hires during the examination period, <i>inspected</i> the new hire checklist and noted it was completed for each new hire in the sample.	No exceptions noted.
2.5	To determine that the policies are understood and agreed to by new hires, an acknowledgement evidencing their understanding and agreement to abide by Avtex policies including the Employee Handbook, Data Privacy Policy, Data Classification Policy, and security policies is required.	For a sample of new hires during the examination period, <i>inspected</i> signed acknowledgements indicating that the new hire read and accepted the Avtex information security policies and procedures.	No exceptions noted.

Personnel Security, Awareness, and Training (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
2.6	In addition, new hires complete security awareness and HIPAA training to help educate employees and contractors on security, data protection, confidentiality, and availability-related risks.	For a sample of new hires during the examination period, <i>inspected</i> training records and noted that HIPAA and security awareness training was completed for each new hire in the sample.	No exceptions noted.
2.7	The Company maintains an intranet site available to all employees that is used to store policies, procedures, and knowledge related to system administration.	<i>Inspected</i> the Company's internal intranet site and noted that it stored Avtex's policies, procedures, and knowledge related to system administration.	No exceptions noted.
2.8	When employees terminate employment with the Company, HR completes a termination checklist in a timely manner.	<p>For a sample of terminated individuals during the examination period, <i>inspected</i> the termination checklist and noted it was completed and validated that all termination activities were performed for each terminated individual in the sample.</p> <p>For a sample of terminated employees during the examination period, <i>inspected</i> termination tickets and supporting review documentation and ascertained that their access was disabled during the deactivation review for each terminated individual in the sample.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Personnel Security, Awareness, and Training (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
2.9	New hires are required to sign a confidentiality agreement, which obligates them to maintain the confidentiality of both Avtex and client data.	For a sample of new hires during the examination period, <i>inspected</i> the employment agreement, including the confidentiality agreement, and noted that each new hire in the sample signed the agreement.	No exceptions noted.
2.10	New hires and new contractors are also required to sign offer letters or contractor agreements, which communicate that appropriate sanctions, up to and including termination of employment, may be applied against individuals who fail to comply with the Company's policies and procedures.	For a sample of new hires during the examination period, <i>inspected</i> the signed offer letter and noted that it communicated Avtex's at-will employment status. For a sample of contractors, <i>inspected</i> the contractor agreement and noted for each contractor in the sample an agreement was signed.	No exceptions noted. No exceptions noted.
2.11	All Avtex's employees are evaluated annually against managerial expectations, general professionalism, technical expectations, areas for growth and improvement, and strengths and contributions.	For a sample of Avtex employees, <i>inspected</i> the annual performance evaluation and noted it was completed for each employee in the sample.	No exceptions noted.
2.12	Avtex has created a training and development policy that outlines employee, management, and Human Resources responsibilities with regard to training.	<i>Inspected</i> the training and development policy and noted it outlined employee, management, and Human Resources responsibilities with regard to employee training and development.	No exceptions noted.

Personnel Security, Awareness, and Training (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
2.13	Annually, Avtex employees and contractors are required to complete security awareness and HIPAA training.	<i>Inspected</i> training records for a sample of employees and contractors and determined that the sample of Avtex employees and contractors completed security awareness training.	No exceptions noted.
2.14	In addition, employees are required to acknowledge Avtex policies including the Code of Conduct, Data Privacy Policy, Data Classification Policy, and security policies annually.	For a sample of employees, <i>inspected</i> signed acknowledgements indicating that the employee read and accepted the Avtex information security policies and procedures.	No exceptions noted.

Network Device Security

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
3.1	The network security policy defines policies requiring the use of VPN and secure protocols for remote access, secure configuration of routers and switches, and the use of ACLs on the firewall.	<i>Inspected</i> the Avtex network security policy and noted that the policy required the use of VPNs and secure protocols for remote access as well as secure configuration of routers, switches, and firewalls.	No exceptions noted.
3.2	The policy is reviewed on a periodic basis by the Vice President, IT Datacenter Ops, and the Information Security Officer.	<i>Inspected</i> the network security policy and noted that it was updated within the last year.	No exceptions noted.
3.3	The IT Department maintains network diagrams which document the network architecture.	<i>Inspected</i> the network diagrams and noted that the diagrams documented the network architecture and included firewalls, routers, and switches.	No exceptions noted.
3.4	The firewalls, routers, and switches employ ACLs and rules to block unauthorized public internet access to the internal network, and a Senior Network Engineer reviews these ACLs on a semi-annual basis.	<i>Inspected</i> a sample of network devices and noted that ACLs were configured to restrict public internet access to the internal network for each device in the sample. <i>Inspected</i> change request documentation and noted that a firewall review and update was completed.	No exceptions noted. No exceptions noted.

Network Device Security (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
3.5	Avtex uses a configuration management tool for infrastructure devices that notifies System Administrators in the event of configuration changes.	<p><i>Inspected</i> output from the network device configuration management tool and noted that it documented changes made to the network device configuration.</p> <p><i>Inspected</i> a notification email from the network device configuration management tool and noted the notification identified that the configuration for a network device changed.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
3.6	Avtex uses RADIUS for authentication to network devices to include routers, switches, and firewalls.	<i>Inspected</i> a sample of network devices and noted that the device was configured to use RADIUS for authentication for each device in the sample.	No exceptions noted.
3.7	Network device access requires entry of a valid user ID and password as well as membership within the Network Admins group. The associated permissions and access capabilities, as appropriate, are based upon legitimate business need.	<p>For a sample of network devices, <i>inspected</i> system configurations and noted that a username and password was required to configure each device in the sample.</p> <p>For a sample of individuals with the ability to configure network devices, <i>inspected</i> associated employee job descriptions and noted that access aligned with job responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Network Device Security (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
3.8	IT Department personnel may also remotely connect to Avtex's network through a VPN connection that requires authentication using a user ID, password, and multi-factor authentication.	For VPN connections used to access the Avtex network remotely, <i>inspected</i> the configuration and noted that users were required to authenticate with a user ID, password, and multi-factor authentication.	No exceptions noted.
3.9	VPNs are configured to transmit data to and from the network securely.	For VPN connections used to access the Avtex network remotely, <i>inspected</i> the configuration and noted that transmissions used TLS v1.2 and AES-256 encryption.	No exceptions noted.

Logical Access

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
4.1	The Company's policies and procedures related to information access management require that access to the Company's systems environment be granted in accordance with business need and restricted to authorized individuals only.	<i>Inspected</i> the Company's policies and procedures and noted that they addressed granting access in accordance with business need.	No exceptions noted.
4.2	The Company has restricted Administrator-level access privileges (i.e., the ability to add, modify, or delete user access) to appropriate Company personnel who require such access to perform their respective job functions.	For a sample of network users with administrator access rights on each Avtex domain and Kaseya, <i>inspected</i> the users technical job role and noted that access was required to perform the users job responsibilities. For a sample of network users with administrator access rights within the CSP portal, <i>inspected</i> the users technical job role and noted that access was required to perform the users job responsibilities.	No exceptions noted. No exceptions noted.
4.3	Network access, as well as access to Kaseya, is controlled by the IT Department and is restricted to authorized personnel.	For a sample of network users on each domain as well as a sample of Kaseya users, <i>inspected</i> the users technical job role and noted that access was required to perform the users job responsibilities.	No exceptions noted.

Logical Access (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
4.4	In order to gain access to the systems environment, personnel must first successfully log in to the Company's Microsoft Windows-based AD network or Kaseya using a valid user ID and password.	<i>Observed</i> a user logging in to the network and noted that the users must first log in to the network before network resources, including client environments, could be accessed.	No exceptions noted.
4.5	Account requests are in the form of a CTN and must include formal approval from a manager.	For a sample of new hires during the examination period, <i>inspected</i> the new hire ticket and noted that each new hire's user access request was approved by a manager.	No exceptions noted.
4.6	User access is granted based on the user's job responsibilities as well as business need.	<i>Inspected</i> the new hire ticket for a sample of new hires during the examination period and noted that access was granted based on the requirements of each new hire's job duties.	No exceptions noted.
4.7	Requests to add new client users to client environments must be approved by an authorized client point of contact, and the user's access level is granted based on the access request.	<i>Inquired</i> with management and noted that there was a process in place to add new client users to client environments. Noted through <i>inquiry</i> that there were no requests to add new client users to client environments. Thus the operating effectiveness of this control could not be tested.	No exceptions noted. No exceptions noted.

Logical Access (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
4.8	When employees terminate employment from the Company, and when contractors complete their work assignments, a system administrator revokes their access in a timely manner.	<i>Inspected</i> termination tickets and determined that system access was revoked in a timely manner for a sample of terminated employees during the examination period.	No exceptions noted.
4.9	When Avtex receives requests to terminate the access of client employees to Kaseya, access is disabled within 24 hours.	<i>Inquired</i> with management and noted that there was a process in place to remove client users from Kaseya. Noted through <i>inquiry</i> that there were no requests to remove client users from Kaseya. Thus, the operating effectiveness of this control could not be tested.	No exceptions noted. No exceptions noted.
4.10	Passwords are established according to a standard, which requires that: a) all user IDs must have a password; b) passwords are user-created and at least eight characters in length; c) passwords must be complex, meaning they must contain upper- and lower-case alphabetic, numeric, and special characters; d) the previous twelve passwords cannot be used; and e) passwords of individuals must be changed at least every 90 days.	<i>Inspected</i> the password policy settings for each Microsoft Active Directory domain as well as Kaseya and noted that the settings enforced password complexity and rules as noted in the control.	No exceptions noted.

Logical Access (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
4.11	Annual entitlement reviews of administrator access within the Avtex environment are performed and access is modified based on the results of the reviews as needed.	<i>Inspected</i> the results of the last entitlement review and noted that the review was completed and included review comments and requested access modifications.	No exceptions noted.
4.12	Avtex clients have access to only their own data and do not have access to any other client's data.	<i>Inspected</i> client user security roles within Kaseya and noted client hosts are separated from one another and access to client hosts was limited to clients and the user did not have access to any other clients' hosts. For a sample of clients, <i>inspected</i> the VLAN configurations and noted that clients were isolated from other clients' virtual machines and data.	No exceptions noted. No exceptions noted.
4.13	Avtex encrypts the hard drives of all employee laptops.	<i>Inspected</i> the Avtex Domain Group Policy and noted workstations were configured to automatically be encrypted.	No exceptions noted.
4.14	Avtex's policies related to media protection address the handling of devices and media that may potentially contain sensitive Company or client data, including PII and ePHI.	<i>Inspected</i> Avtex's security policies and noted that policies were in place governing the handling of media that contained sensitive data.	No exceptions noted.

Logical Access (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
4.15	Avtex defines specific requirements for hardware and data disposal in its security policies.	<i>Inspected</i> Avtex's security policies and noted that hardware and data destruction policies were defined.	No exceptions noted.
4.16	All electronic equipment is wiped of all data or is physically destroyed by a well-known third party who specializes in secure media destruction.	<i>Inspected</i> certificates of destruction and noted that Avtex employed a third party who specialized in secure media destruction to physically destroy or wipe electronic media.	No exceptions noted.
4.17	Employee workstations are configured to enable a screensaver after a modest period of inactivity, and a password is required to regain access to the workstation.	<i>Inspected</i> domain policy configurations and noted that Avtex workstations were configured to enable a screensaver after a period of inactivity, and a password was required to regain access to the workstation.	No exceptions noted.

Protection from Malicious Software

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
5.1	Acceptable use language within the employee handbook prohibits the download or importation of programs, files, or documents into the Company's systems environment except as authorized by Avtex.	For a sample of new hires during the examination period, <i>inspected</i> the employee handbook and noted that it was signed and that the new hires acknowledged the acceptable use language.	No exceptions noted.
5.2	The policy requires that all images deployed on servers and workstations are up-to-date on security patches.	<i>Inspected</i> the System Hardening policy and noted that it required all servers and workstations to be up-to-date on security patches.	No exceptions noted.
5.3	Avtex has created an antivirus policy which requires that Avtex deploy antivirus software on its workstations and servers which may access or support clients' system environments.	<i>Inspected</i> the Antivirus policy and noted that it required that Avtex to deploy antivirus software on servers and workstations that access or support clients' system environments.	No exceptions noted.
5.4	Avtex has configured the antivirus software to update the antivirus signature definitions automatically and perform regularly scheduled scans on all employee workstations and hosted servers.	<i>Inspected</i> the Kaseya configuration and noted current antivirus software was automatically applied to workstations and servers.	No exceptions noted.

Protection from Malicious Software (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Tests
5.5	Avtex patches internal workstations, managed services servers, and internal servers as needed.	<p><i>Inspected</i> the Kaseya security policy and noted security patches for workstations, managed services servers, and internal servers are automatically updated.</p> <p>For managed services servers that are not automatically patched at the request of the client, <i>inspected</i> a sample of servers and noted security patches were current.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
5.6	For managed servers, Avtex audits all patches and patching details monthly and updates the server and patching details as needed.	For a sample of months, <i>inspected</i> the results of the patching audits and noted that the patching audit for managed servers was performed.	No exceptions noted.
5.7	Avtex follows up on potential issues as needed and takes corrective action to prevent unauthorized access.	<p><i>Inspected</i> the intrusion detection system and noted it was in place and monitoring network activity.</p> <p>Through <i>inquiry</i>, noted that suspicious network activity was followed up on and corrective action was taken to block unauthorized access as needed.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Physical Access

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
6.1	The building is unlocked from 6:00 am to 7:00 pm, Monday through Friday, 7:00 am to 3:00 pm on Saturday, and at all other times, the building is locked, and a card key is required to enter.	<i>Inquired</i> of Avtex management and noted that the main doors to the building where the office suite was located were locked outside of the hours as described.	No exceptions noted.
6.2	Avtex's office suite has one main entrance with a receptionist, which is physically secured by a card key system and access is provided only to authorized personnel.	<i>Observed</i> the office suite and noted that there was one main entrance to the premises with a receptionist during office hours. <i>Observed</i> the office suite and noted that all entrances required valid key cards to gain access. For a sample of card key holders, <i>inspected</i> the HR current employee list and noted that the card key was issued to only authorized personnel.	No exceptions noted. No exceptions noted. No exceptions noted.

Physical Access (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
6.3	All visitors are received by an authorized employee who must monitor the visitor while they are in the office.	Due to COVID-19 restrictions, Avtex employees began to work remotely in April 2020, and there have not been visitors to the Avtex offices. Therefore, this control did not operate during the period.	No exceptions noted.
6.4	Physical access to the server room is restricted to authorized IT Department and management personnel.	<i>Observed</i> the server room entrance and noted that the entrance required a valid key card to gain access. For all card key holders with access to the server room, <i>inspected</i> the key card access report and noted that only appropriate personnel who required the access for their job role were issued key cards.	No exceptions noted. No exceptions noted.
6.5	When personnel terminate employment from Avtex, their card key is collected on the individual's last day of work and is disabled in the card key system.	For a sample of individuals who terminated employment during the examination period, <i>inspected</i> the key card system cardholder list and noted that each terminated individual's key card was disabled or deleted.	No exceptions noted.
6.6	Only authorized management and IT Department personnel may contact CoLogix or vXchnge on behalf of Avtex and request services.	<i>Inspected</i> the CoLogix and vXchnge authorized contact lists and noted that all individuals were authorized Avtex IT Department employees.	No exceptions noted.
6.7	Avtex also restricts physical access to the Avtex cabinets within the CoLogix and vXchnge data centers to authorized employees only.	<i>Inspected</i> the CoLogix and vXchnge access control listing and noted that all individuals were authorized Avtex IT Department employees.	No exceptions noted.

Data Transmission

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
7.1	SFTP data connections between Avtex and clients use industry-standard, strong encryption algorithms.	<i>Inspected</i> the SFTP server configuration and noted that connections were secured with industry-standard, strong encryption algorithms.	No exceptions noted.
7.2	Kaseya incorporates the use of AES 256-bit encryption to encrypt data submitted by Avtex clients through Kaseya.	<i>Inspected</i> Kaseya security and compliance documentation and noted used 256-bit AES encryption to securely transmit data.	No exceptions noted.
7.3	For authorized Avtex employees and authorized clients, Avtex provides secure VPN access.	<i>Inspected</i> the VPN client and server configurations and noted that VPN connections to the Avtex network were encrypted. <i>Inspected</i> a sample of client site-to-site VPN connections and noted that AES-256 encryption was used for each client in the sample.	No exceptions noted. No exceptions noted.
7.4	Avtex restricts access to each client home directory to only a single authorized client user and locks the user to only that home directory.	<i>Inspected</i> the configuration of the SFTP server and noted that access to client directories was restricted to the single authorized client user and users were locked to their home directory.	No exceptions noted.

Monitoring

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
8.1	Avtex's policies related to logging and monitoring of information systems activity and health require the collection and review of information systems activity in audit logs, access reports, and security incident tracking reports.	<i>Inspected</i> Avtex's system monitoring and maintenance policy and noted that it addressed information system activity logging, monitoring, and reporting.	No exceptions noted.
8.2	Avtex monitors and logs information system activity for their clients' environments as well as the core infrastructure shared among clients.	<i>Inspected</i> monitoring dashboards and audit records and noted that Avtex monitored and logged information system activity related to its core infrastructure and client production environments.	No exceptions noted.
8.3	Avtex's MS personnel review the IT infrastructure logged events in real time and alert on specific events and issues related to key IT infrastructure components.	<i>Inspected</i> the monitoring tool configurations and generated alerts and noted that IT infrastructure events were monitored, and alerts were configured to notify system administrators in the event that an issue arises.	No exceptions noted.
8.4	Issues that require additional follow-up are entered into the ticketing system, appropriately acted upon, and monitored to resolution.	<i>Inspected</i> a sample of tickets and noted that issues identified through the use of monitoring tools were documented, addressed, and resolved in a timely manner.	No exceptions noted.
8.5	Avtex obtains and reviews the SOC 2 report provided by CoLogix, vXchnge, Microsoft Azure, and Genesys to determine whether controls are designed and operating effectively.	<i>Inspected</i> evidence and noted that Avtex obtained and reviewed the SOC 2 report for CoLogix, vXchnge, Microsoft Azure, and Genesys.	No exceptions noted.

Incident Response and Contingency Planning

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
9.1	Avtex has established and implemented a security incident management policy and security incident management procedures to be activated in the event a security or availability incident occurs.	<p><i>Inspected</i> the security incident management policy and noted that it addressed the required elements of incident response.</p> <p><i>Inspected</i> the security incident management procedures document and noted that it defined appropriate actions to follow in the event of an incident.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
9.2	The security incident management policy and procedures are reviewed and updated annually and more frequently based upon incident outcomes and lessons learned, as appropriate.	<i>Inspected</i> the document review history and determined that the security incident management policy and security incident management procedures were reviewed and approved within the past year.	No exceptions noted.
9.3	Avtex maintains a record of all security and availability incidents within their ticketing system. Of the low, medium, high/emergency ticket prioritization categories, security and availability incidents are categorized as high/emergency.	For a sample of incident tickets, <i>inspected</i> and noted that security and availability incidents were categorized as High or Emergency.	No exceptions noted.
9.4	Incidents and problems logged on behalf of clients are documented, addressed, and resolved in a timely manner.	Through <i>inspection</i> of a sample of incident tickets, noted that the tickets were documented, addressed, and resolved in a timely manner.	No exceptions noted.

Incident Response and Contingency Planning (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
9.5	Avtex maintains a backup copy of its essential production systems, including client data, at an offsite location.	Through <i>inspection</i> , noted that an offsite backup solution existed and backups were configured to occur daily and replicated to an offsite location.	No exceptions noted.
9.6	Backup data is encrypted at rest.	Through <i>inspection</i> of system configurations, noted that backup data was encrypted at rest.	No exceptions noted.
9.7	Disaster recovery scenarios are tested in any year that a disaster was not declared.	<p><i>Inspected</i> results of a disaster recovery exercise and noted that an applicable scenario was tested and discussed.</p> <p><i>Inspected</i> results of a security incident response exercise and noted that an applicable scenario was tested and discussed.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
9.8	In the event of a breach, Avtex is required to notify each client affected by the breach in a timely manner and in conformity with the contractual obligations in place.	<p><i>Inspected</i> the security incident management policy and procedures, the data classification policy and the data privacy policy and noted that Avtex's process was to notify each client affected by a breach in a timely manner.</p> <p><i>Inquired</i> of management and noted that no breaches of ePHI occurred during the audit period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

Incident Response and Contingency Planning (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
9.9	Avtex's business associate agreement with subservice organizations and contractors obligates such organizations to report breaches, if any, to Avtex in a timely manner.	<i>Inspected</i> the Avtex business associate agreement and noted that it obligated the subservice organization or contractor to report breaches to Avtex in a timely manner.	No exceptions noted.

Change Management

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
10.1	To facilitate a structured change management process, Avtex has documented procedures which outline the requirements and appropriate protocols for enacting changes to key/critical information systems.	<i>Inspected</i> the change management policy and noted that it outlined the process for documenting, testing, evaluating, and authorizing changes prior to implementation.	No exceptions noted.
10.2	A change request is submitted via an electronic change request form on ThePoint.	<p><i>Inspected</i> a sample of changes during the examination period and noted that a formal request was submitted for each change.</p> <p>For a sample of changes during the examination period, <i>inspected</i> change tickets and ascertained that risk and security implications were considered.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
10.3	The CAB meets weekly to review and approve change requests except during change freeze periods.	<p><i>Observed</i> a weekly CAB meeting and noted that changes were discussed and approved.</p> <p><i>Inspected</i> a sample of CAB meeting minutes and noted CAB meetings occurred weekly.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
10.4	Changes must be authorized in accordance with the decision-making responsibility matrix prior to implementation in production.	<i>Inspected</i> evidence that a sample of changes during the examination period were authorized in accordance with the decision-making responsibility matrix.	<p>Approvals for two (2) of 25 changes reviewed could not be provided.</p> <p>Management Response: See section VI.</p>

Change Management (continued)

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
10.5	Test activities are documented in the request for change ticket.	For a sample of changes during the examination period, <i>inspected</i> change tickets and noted that test activities were documented.	No exceptions noted.
10.6	For changes that impact Avtex's commitments and requirements relevant to security and availability, Avtex communicates the potential security and availability impact to those users in a timely manner.	Through <i>inspection</i> of a sample of customer-impacting changes during the examination period, noted that Avtex communicated information about the change to the client prior to deployment.	No exceptions noted.

Control Activities

Ref	Controls Specified by Avtex	Testing Performed by Linford & Company	Results of Testing
11.1	Avtex has developed a set of policies that establish expected behavior with regard to the Company's control environment.	<i>Inspected</i> the code of conduct policy, ethics policy, and IT related policies and noted that they communicated the expected behavior to employees regarding security and availability.	No exceptions noted.
11.2	Avtex management also segregates responsibilities and duties across the organization and within the infrastructure environment to mitigate risks to the services provided to its clients.	<i>Inspected</i> the Avtex organizational chart, system configurations, and role assignments and noted that responsibilities and duties were segregated within the organization and within the infrastructure environment.	No exceptions noted.

Section V – SOC 2 Requirements and Controls

The Avtex management team is responsible for establishing and maintaining effective controls over its hosting and managed services. The controls are designed to provide reasonable assurance to Avtex’s management and the board of directors that the following SOC 2 Security and Availability control criteria are achieved.

In the table that follows, the columns have the following meaning:

SOC 2 Criteria – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the Trust Services Criteria.

Requirement(s) – This column contains the text of the criterion (requirement) directly from the Trust Services Criteria.

Reference – This column contains the reference to the control activities in Section III, *Description of Control Activities Prepared by Management*, which are relevant to the achievement of the criterion.

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in Section III, *Avtex Solutions, LLC’s Description of its Hosting, Contact Center Support, and Managed Services*, address the SOC 2 control criteria.

Many of the criteria used to evaluate a system are shared amongst security, availability, processing integrity, and confidentiality. For example, the criteria related to risk management apply to the security, availability, processing integrity, and confidentiality. As a result, the criteria for the security, availability, processing integrity, and confidentiality criteria are organized into the criteria that are applicable to all four criteria (Common Criteria). The Common Criteria constitute the complete set of criteria for the security criteria. The criteria in A1.1 through A1.3 in the table that follows constitutes the complete set of the criteria for the availability criteria.

Common Criteria / Security Criteria

Security. The trust services criteria relevant to security address the need for information and system to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.0 Common Criteria Related to Control Environment

SOC 2 Criteria	Requirement(s)	Reference
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	11.2
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.6, 1.12, 1.14
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.2, 1.16, 1.17, 8.3

CC1.0 Common Criteria Related to Control Environment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	2.2, 2.6, 2.7, 2.11, 2.12
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.2, 1.3, 1.4, 1.18, 2.3, 2.5, 2.9, 2.10, 2.11, 2.14, 5.1

CC2.0 Common Criteria Related to Communication and Information

SOC 2 Criteria	Requirement(s)	Reference
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1, 2.3, 2.4, 2.7, 2.11, 3.2, 3.3
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.	1.1, 1.3, 1.4, 2.5, 2.9, 2.10, 2.13, 3.2, 5.1
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	1.9, 1.11, 9.8, 9.9, 10.6

CC3.0 Common Criteria Related to Risk Assessment

SOC 2 Criteria	Requirement(s)	Reference
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	1.5-1.8
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.	1.5-1.8
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	1.5-1.8
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	1.5-1.8

CC4.0 Common Criteria Related to Monitoring Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	1.12, 1.15, 11.1
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.	4.11

CC5.0 Common Criteria Related to Control Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	5.1, 5.2
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.1, 5.2
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.	1.1, 1.3, 1.4, 2.5, 3.1, 3.2, 4.1, 4.14, 5.3, 8.1, 9.1, 9.2, 10.1, 11.2

CC6.0 Common Criteria Related to Logical and Physical Access Controls

SOC 2 Criteria	Requirement(s)	Reference
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.	1.10, 3.4, 3.6, 3.7, 3.8, 3.9, 4.3, 4.4, 4.10, 4.12, 4.13, 4.17, 9.6
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.	2.4, 4.2, 4.5-4.9
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.	1.10, 2.4, 2.8, 3.6, 3.7, 3.8, 4.2-4.9, 4.11, 4.14
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.	2.8, 4.2, 4.3, 4.11, 6.1-6.7, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs
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.	4.15, 4.16, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs

CC6.0 Common Criteria Related to Logical and Physical Access Controls (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	3.1, 3.4, 4.13, 7.1-7.3, 9.6
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.	3.1, 3.4, 3.8, 3.9, 4.13, 7.1-7.4
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.	5.2-5.7

CC7.0 Common Criteria Related to System Operations

SOC 2 Criteria	Requirement(s)	Reference
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.	1.13, 3.5, 8.2-8.4, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs
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.	1.13, 3.5, 8.2-8.4, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs
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.	3.5, 8.3, 8.4, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs
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.	9.1, 9.3, 9.4, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	9.1, 9.4, vXchnge CSOCs, CoLogix CSOCs, Azure CSOCs, & Genesys CSOCs

CC8.0 Common Criteria Related to Change Management

SOC 2 Criteria	Requirement(s)	Reference
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.	3.5, 10.1-10.6

CC9.0 Common Criteria Related to Risk Mitigation

SOC 2 Criteria	Requirement(s)	Reference
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	1.5-1.8
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	1.5-1.8, 8.5

Availability Controls

Availability Principle: The system is available for operation and use as committed or agreed.

Note: The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems) but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

Additional Criteria for Availability

SOC 2 Criteria	Requirement(s)	Reference
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.	8.2-8.4, 9.5
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.	9.3, 9.5
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	9.7

Section VI – Other Information Provided by Avtex That Is Not Covered by the Service Auditor’s Report

Management Responses to Section IV Results of Testing

Change Management

Control 10.4: Agreed.

Agreed. Management has put steps in place so that approvals for changes made to the production environment are documented consistently for each change.

One change was reviewed and approved by the Change Advisory Board but was not documented in the approval request to the VP of IT for the period. An additional review step was added to the Change Management process to determine that all changes reviewed and approved by the Change Advisory Board are documented in management approval requests sent to the VP of IT.

One change was a recurring change for monthly, scheduled security patching and occurred during an end of year change freeze. Engineers were provided additional training on the existing Change Management Policy and the requirement to receive pre-approval for security and SLA driven changes that occur during changes freezes.