



REPORT OF AVAIL TECHNOLOGIES INC.'S ENTERPRISE TRANSIT MANAGEMENT SOFTWARE
SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS
CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY
THROUGHOUT THE PERIOD FROM APRIL 1, 2024 TO MARCH 31, 2025



Avail Technologies, Inc. – SOC 2 Type 2 Table of Contents

Acronym Table	2
Section 1: Independent Service Auditor's Report	3
Section 2: Assertion of the Management of Avail Technologies, Inc.	8
Section 3: Avail Technologies Inc.'s Description of its Enterprise Transit Management Software	
System Throughout the Period from April 1, 2024 to March 31, 2025	11
Purpose and Scope of Report.....	12
System Description	12
Company Overview and Services Provided.....	12
Principle Service Commitments and System Requirements	13
Infrastructure	13
Software	14
People	15
Procedures	15
Data.....	15
System Boundaries	16
Significant Changes Throughout the Examination Period	16
Subservice Organizations	16
Control Environment	17
Integrity and Ethical Values	18
Commitment to Competence	18
Organizational Structure	18
HR Policies and Practices.....	19
Risk Assessment.....	19
In-Scope Trust Service Categories	19
Security	20
Availability	20
Confidentiality.....	20
Trust Service Categories and Related Control Activities	20
Selection and Development of Control Activities	20
Information and Communication	20
Information Systems	20
Communication	21
Monitoring.....	21
User Entity Controls	21
Section 4: Trust Services Categories, Criteria, Related Controls, and Tests of Controls.....	23
Testing Approach	24
Sampling Approach	24
Trust Services Security, Criteria, Related Controls, and Tests of Controls	25

Acronym Table

◇ AD	Active Directory
◇ AICPA	American Institute of Certified Public Accountants
◇ API	Application Programming Interface
◇ AT	Attestation Standard
◇ AV	Antivirus
◇ Azure	Microsoft Azure
◇ CAD/AVL	Computer-Aided Dispatch / Automatic Vehicle Location
◇ CEO	Chief Executive Officer
◇ The “Company” or Avail	Avail Technologies, Inc. or the “Organization”
◇ CI/CD	Continuous Integration and Continuous Delivery/Deployment
◇ COO	Chief Operating Officer
◇ COSO	Committee of Sponsoring Organizations
◇ CRM	Customer Relationship Management
◇ CSA	Cloud Security Alliance
◇ CTO	Chief Technology Officer
◇ DC	Description Criteria
◇ DevOps	Development and Operations
◇ ERP	Enterprise Resource Planning
◇ ETMS	Enterprise Transit Management Software
◇ EULA	End-User License Agreements
◇ FAQ	Frequently Asked Questions
◇ HR	Human Resources
◇ HTTPS	Hypertext Transfer Protocol Secure
◇ ID	Identification
◇ IDS	Intrusion Detection System
◇ IP	Internet Protocol
◇ IT	Information Technology
◇ LLC	Limited Liability Company
◇ MDM	Mobile Device Management
◇ MDR	Managed Detection Response
◇ MFA	Multi-Factor Authentication
◇ OS	Operating System
◇ PaaS	Platform-as-a-Service
◇ PIM	Product Information Management
◇ QA	Quality Assurance
◇ RBAC	Role-based Access Control
◇ SaaS	Software-as-a-Service
◇ SDLC	System Development Life Cycle
◇ SLA	Service Level Agreement
◇ SOC	System and Organizational Control
◇ SQL	Structured Query Language
◇ SSH	Secure Socket Shell
◇ SSL	Secure Sockets Layer
◇ TLS	Transport Layer Security
◇ TSC	Trust Service Category
◇ TSP	Trust Service Principle
◇ US	United States
◇ VM	Virtual Machine
◇ VPC	Virtual Private Cloud
◇ VPN	Virtual Private Network

Section 1: Independent Service Auditor's Report



Independent Service Auditor's Report on the Description of Avail Technologies, Inc.'s Enterprise Transit Management Software System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, and Confidentiality

To: Management of Avail Technologies, Inc.:

Scope

We have examined Avail Technologies, Inc.'s (the Company, Organization, or Avail Technologies) accompanying description of its Enterprise Transit Management Software System (System) found in Section 3 titled, "Avail Technologies' Description of its Enterprise Transit Management Software System Throughout the Period from April 1, 2024 to March 31, 2025 (description), based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (description criteria) and the suitability of the design and operating effectiveness of the controls stated in the description throughout the period from April 1, 2024 to March 31, 2025, to provide reasonable assurance that Avail Technologies' service commitments and system requirements surrounding its Enterprise Transit Management Software System were achieved based on the Trust Services Criteria relevant to security, availability, and confidentiality (applicable Trust Services Criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (AICPA, Trust Services Criteria). The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the Company's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of the Company'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.

Avail Technologies uses subservice organizations Azure and OneTrust to host the production infrastructure and provide continuous security and compliance monitoring, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Avail Technologies, to achieve Avail Technologies' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Avail Technologies' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Avail Technologies' 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 organization controls.

Service Organization's Responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. In Section 2, the Company has provided its assertion titled, "Assertion of the Management of Avail Technologies, Inc." (assertion) about the description and suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, selecting the applicable Trust Services Criteria and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- ◇ Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- ◇ Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- ◇ Performing procedures to obtain evidence about whether the description is presented in accordance with 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 has 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.

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

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 each individual user may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

The Company's description of its System discusses the following controls that did not operate within the period from April 1, 2024 to March 31, 2025:

- ◇ Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the Organization's privacy and confidentiality commitments.
- ◇ A vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.

Because the controls did not operate within the stated period, we were unable to test, and did not test, the operating effectiveness of the controls as evaluated using the related Trust Services Criteria.

Opinion

In our opinion, in all material respects, based on the description and the applicable Trust Services Criteria:

- a) The description presents the Company's System that was designed and implemented throughout the period from April 1, 2024 to March 31, 2025, in accordance with the description criteria.
- b) The controls stated in the description were suitably designed throughout the period from April 1, 2024 to March 31, 2025 to provide reasonable assurance that the Company'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 organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period.
- c) The controls stated in the description operated effectively throughout the period April 1, 2024 to March 31, 2025 to provide reasonable assurance that the Company'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 the Company's controls operated effectively throughout the period.

Restricted Use

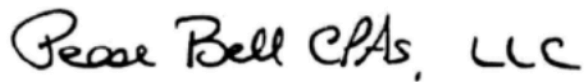
This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Company, user entities of the Company's System during some, or all, of the period from April 1, 2024 to March 31, 2025, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- ◇ The nature of the service provided by the service organization.

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

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

Pease Bell CPAs, LLC

A handwritten signature in black ink that reads "Pease Bell CPAs, LLC". The script is cursive and fluid, with the letters "P", "B", "C", and "L" being particularly prominent.

April 16, 2025

Akron, Ohio

Section 2: Assertion of the Management of Avail Technologies, Inc.



Assertion of the Management of Avail Technologies, Inc.

We have prepared the accompanying description of Avail Technologies, Inc.'s (the Company, Organization, or Avail) Enterprise Transit Management Software system (System) titled, "Avail Technologies, Inc.'s Enterprise Transit Management Software System Throughout the Period from April 1, 2024 to March 31, 2025" (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Enterprise Transit Management Software system that may be useful when assessing the risks arising from interactions with Avail Technologies' system, particularly information about system controls that Avail Technologies has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security, availability, and confidentiality (applicable Trust Services Criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Avail Technologies uses subservice organizations to host the production infrastructure and to provide continuous security and compliance monitoring. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Avail Technologies, to achieve Avail Technologies' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Avail Technologies' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Avail Technologies' 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 Avail Technologies, to achieve Avail Technologies' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the service organization's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

- 1) The description presents Avail Technologies, Inc.'s Enterprise Transit Management Software system that was designed and implemented throughout the period from April 1, 2024 to March 31, 2025 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period from April 1, 2024 to March 31, 2025 to provide reasonable assurance that Avail Technologies' service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Avail Technologies' controls throughout that period.
- 3) The controls stated in the description operated effectively throughout the period from April 1, 2024 to March 31, 2025 to provide reasonable assurance that Avail Technologies' service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Avail Technologies' controls operated effectively throughout that period.

- 4) The Company's description of its system discusses the following controls that did not operate within the period from April 1, 2024 to March 31, 2025 due to no occurrence of the activity to test the operating effectiveness:
- ◇ Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the Organization's privacy and confidentiality commitments.
 - ◇ A vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.

/s/ Walt Timblin, Jr.

Information Technology Lead

Avail Technologies, Inc.

April 16, 2025

**Section 3: Avail Technologies Inc.'s Description of its Enterprise
Transit Management Software System
Throughout the Period from April 1, 2024 to March 31, 2025**

Purpose and Scope of Report

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of Avail Technologies' controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user entities, is intended to assist user auditors in planning the audit of the user entities and in assessing control risk for assertions of the user entities that may be affected by policies and procedures of Avail Technologies, Inc.'s Enterprise Transit Management Software System.

This report describes the system and control structure of Avail Technologies as it relates to Avail Technologies Inc.'s Enterprise Transit Management Software System. The report is intended to assist user entities and their independent auditors in determining the adequacy of the internal controls that are outsourced to Avail Technologies and are relevant to their internal control structures as they relate to security, availability, and confidentiality risks. This document was prepared in accordance with the guidance contained in the AICPA AT Section 101 – Attest Engagements.

Avail Technologies uses subservice organizations Azure and OneTrust to host the production infrastructure and to provide continuous security and compliance monitoring, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Avail Technologies, to achieve Avail Technologies' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Avail Technologies' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Avail Technologies' controls. The description does not disclose the actual controls at the subservice organizations.

This description is intended to focus on the internal control structure of Avail Technologies that is relevant to only users of Avail Technologies, Inc.'s Enterprise Transit Management Software System and does not encompass all aspects of the services provided or procedures followed by Avail Technologies.

System Description

Company Overview and Services Provided

Founded in 1999, Avail Technologies is a software product company headquartered in State College, Pennsylvania. Avail Technologies partners with customers to create solutions with an Enterprise Transit Management Software System. Avail Technologies is recognized as the industry's leading provider of its technology solutions for mid-sized transit operators throughout the United States. Because of the unique market focus, Avail Technologies' dedicated team is firmly positioned to better serve transit operators by providing industry-leading products, proven engineering processes, and the highest degree of integrity possible.

Services Provided

Avail Technologies offers the myAvail product – an Enterprise Transit Management Software System which includes dispatch, scheduling, yard and pull-out management, paratransit support, and other features. By design, Avail Technologies has remained a mid-sized Company that stays focused on providing cost-effective engineering services and cutting-edge technologies to the target market of transit operators with medium-sized fleets. The targeted approach allows for the understanding of property needs and transit operators. To date, Avail Technologies is the only systems integrator that has limited pursuits to a specific market segment to the transit software market. The myAvail product offers the only enterprise-level transit software solution. Avail Technologies' experience allows for the design, development, and adoption of technology solutions that provide the features and benefits to improve daily transit operations and to enhance the rider experience.

Additional features of the myAvail ETMS System include:

- | | |
|---|-------------------------|
| ◇ Enterprise-level advanced transit management solution | ◇ CAD/AVL |
| ◇ Role-based user interface | ◇ Centralized database |
| | ◇ Business intelligence |

Principle Service Commitments and System Requirements

Avail Technologies designs its processes and procedures related to its Enterprise Transit Management Software System to meet its objectives. Those objectives are based on the service commitments that Avail Technologies makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Avail Technologies has established for the services.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the product offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- ◇ Security principles within the fundamental designs of the ETMS System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role; and
- ◇ Use of encryption technologies to protect customer data both at rest and in transit.

Availability commitments to user entities are documented in client agreements. Availability commitments are standardized and include, but are not limited to, the following:

- ◇ Managing software, servers (including storage), network, internet, and infrastructure capacity as is necessary to provide a commercially reasonable level of performance of the services;
- ◇ Meeting Company objectives through the authorization, design, development, and monitoring of data backup processes and recovery infrastructure; and
- ◇ Support coverage, hours of availability, response times and resolution times.

Confidentiality commitments to user entities are documented in client agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- ◇ Confidential data is prohibited from being used or stored in non-production systems or environments.

Avail Technologies establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Avail Technologies' system policies and procedures, system design documentation, 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 the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Enterprise Transit Management Software System.

Infrastructure

Avail Technologies utilizes Azure's PaaS which provides all the infrastructure to support web apps, including storage, web and application servers, networking resources, operating systems, development tools, database management, and business analytics. The primary infrastructure used to deliver the Enterprise Transit Management Software System consists of Azure virtual machine scale sets which are hosted in the Azure East US, Central US, West US, and West US 2 regions. The application is secured using VPN tunnel authentication, with identity and access management being managed through Azure AD.

The application servers are hosted in the Azure cloud and run on Microsoft OS. They are optimized for performance and stability and are continuously monitored to ensure that they are running optimally. Azure Security Groups are used to control inbound and outbound network traffic to the application servers, allowing administrators to manage access based on source IP addresses, protocol, and port. This provides an additional layer of security to the application by limiting access to only authorized users and applications.

Microsoft SQL server databases and Azure Blob storage are used to store data. The databases are encrypted using strong encryption technologies. Additionally, backups are performed using Azure Snapshots, allowing for easy restoration of the database in the event of loss or corruption. To ensure that the application is always available to users, a load balancer is in place to manage and distribute incoming traffic evenly across the application servers.

Azure acts as a full PaaS provider. All hardware management is completely reserved to Azure facilities, including housing of VMs, networking of machines, and virtualization of hardware to customers. The Azure infrastructure is designed and managed in accordance with security compliance standards and industry best practices including SOC 2 security, availability, confidentiality, and processing integrity, and privacy compliance, and CSA Star compliance.

Software

The following provides a summary of systems used to deliver the Enterprise Transit Management Software System:

- ◇ Arctic Wolf provides 24/7 managed detection and response from the Triage Team, containment and remediation from the Concierge Team, and an Incident Response retainer for the cyber insurance carrier.
- ◇ Azure AD is used as the cloud-based identity and access management service that facilitates user access to external resources, such as Microsoft 365, the Azure portal, and many of other SaaS applications.
- ◇ Azure DevOps is used as a set of developer tools and services provided by Azure. It offers agile planning tools, CI/CD for any platform, private repositories, manual and exploratory testing, universal package repository, and other tools.
- ◇ Azure PIM is used to manage, control, and monitor access to important resources in the environment. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.
- ◇ Bitwarden's password manager solution is used to secure passwords, endpoints, remote access, and privileged access. All Azure customer local Admin passwords are changed and rotated within Bitwarden by the Upgrades Team. All employees have Bitwarden to secure their own and shared passwords.
- ◇ CyberFOX AutoElevate is used to elevate privileges to known, trusted applications that require them, control the application usage, and log and report on privileged activities using security tools already in place.
- ◇ KnowBe4 provides an integrated platform for security awareness training and simulated phishing attacks.
- ◇ Microsoft Dynamics 365 portal directly syncs all the information from the CRM portal.
- ◇ Microsoft Dynamics provides a CRM solution for tailored experiences to customers, partners, and employees for improved sales, marketing, and service management.
- ◇ Microsoft Intune (Firewall & Antivirus) is used to manage user access and simplify application and device management across many devices, including mobile devices, desktop computers, and virtual endpoints.
- ◇ Microsoft Office 365 is used as the identity provider to manage authentication and access controls to production systems and applications.
- ◇ Microsoft Office products are used as corporate productivity tools such as Word, Excel, Outlook, and Teams.
- ◇ Microsoft Teams is used as an internal communication tool.
- ◇ OneTrust provides information security and compliance-accessible solutions.
- ◇ Pendo is used as a product-analytics application to embed content regarding FAQs and training material accessible within the ETMS System.
- ◇ Trend Micro Cloud One Endpoint Security is used to protect endpoints, servers, and cloud workloads through unified visibility, management, and role-based access control.

- ◇ Trend Micro is used as an endpoint security solution to stop ransomware, phishing, and advanced malware attacks in their tracks. Trend Micro combines the industry's leading malware detection and exploit protection with MDR to secure the entire ecosystem.

People

People involved in the operation and use of the system are:

- ◇ CEO, who is responsible for leading and overseeing overall Company operations, including finance, HR, sales, marketing, and managing the day-to-day operations of Avail Technologies.
- ◇ CTO, who is responsible for oversight of IT related hardware, software, configuration, and security.
- ◇ COO, who is responsible for helping customers achieve their strategic goals by providing expert consulting, technical solutions, project planning services, and leadership for cross-functional teams to implement solutions which improve quality and efficiency while reducing expenses.
- ◇ Director of Products, who is responsible for product implementation, customer retention, support, and other project management duties.
- ◇ Director of Staff Engineers, who is responsible for product development and current product maintenance.
- ◇ Director of Development, QA/Test, IT, who is responsible for overseeing data management, creating data strategies, and improving data quality.

Procedures

Executive and Operations Management personnel maintain documented operating procedures involved in the operation of Avail Technologies, Inc.'s Enterprise Transit Management Software System that include:

- | | |
|--|--------------------------------------|
| ◇ Acceptable Use Policy | ◇ HR Security Policy |
| ◇ Access Control Policy | ◇ Incident Management Plan |
| ◇ Asset Management Policy | ◇ Information Security Policy |
| ◇ Business Continuity & Disaster Recovery Policy | ◇ Network Security Policy |
| ◇ Backup & Restoration Policy | ◇ Operations Security Policy |
| ◇ Change Management Policy | ◇ Physical Security Policy |
| ◇ Corporate Ethics Policy | ◇ Risk Management Policy |
| ◇ Cryptography Policy | ◇ Secure Software Development Policy |
| ◇ Data Management Policy | ◇ Vendor Management Policy |
| | ◇ Workstation Security Policy |

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which Avail Technologies strives to achieve its business objectives. Avail Technologies has applied a risk management approach to the Organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved, when necessary, to meet the applicable Trust Services Criteria and the overall objectives of the Organization.

The Avail Technologies control procedures which have been designed to meet the applicable Trust Services Criteria are included in Section 4 of this report to eliminate the redundancy that would result from listing the procedures in this section.

Data

Access controls and privileges are distributed to Avail Technologies employees and users of the Enterprise Transit Management Software System using the method of least privileges. Applications have enabled RBAC. Customer data stored within the Company's data stores are encrypted at rest. IT follows the new hire and termination procedures for granting new user access to in-scope systems and revoking access in a timely manner when required. An inventory of production systems is in place and maintained. Any access to network systems or production datastores requires a unique username and password or authorized SSH keys prior to being granted access.

Formal retention and disposal procedures are in place and secure disposal techniques are utilized when purging or deleting data and information. Avail uses an IDS to provide continuous monitoring of its network and early detection of potential security breaches. Production systems can only be remotely accessed by authorized employees possessing a valid MFA token. An MDM system is in place to centrally manage mobile devices supporting the system service.

Avail Technologies' network is located behind Azure Security Groups and the network is segmented to prevent unauthorized access to customer data. The Company's production systems are only accessible by authorized employees over an encrypted connection. Any data or information that is passed over public networks is redirected to HTTPS that is encrypted by TLS 1.2 or stronger ciphers.

The Avail Technologies corporation has data classification policies and procedures to identify confidential information in the system and to define instructions for handling and labelling confidential information. Avail Technologies' cloud provider Key Management Service is utilized to manage encryption keys. Access to production access keys is restricted to authorized individuals.

System Boundaries

System boundaries, pertaining to the collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements. The scope of this report is limited to the in-scope systems hosted in Azure.

Significant Changes Throughout the Examination Period

There were no significant changes that occurred throughout the examination period.

Subservice Organizations

Avail Technologies relies on subservice organizations to create efficiencies in the Enterprise Transit Management Software System. Below is a list of relevant subservice organizations and responsibilities expected to be met by those organizations. Avail Technologies monitors the service commitments made by the subservice organizations in an annual vendor management program. Avail Technologies obtains attestation reports, or other relevant information, and reviews the controls and test results to help ensure the subservice organization's service commitments are met. Remediation plans and monitoring timelines are implemented if testing exceptions were discovered in Avail Technologies' review of the attestation reports.

Azure

Avail Technologies uses Azure to host their Enterprise Transit Management Software System which utilizes Azure services for the management of data and processes. Azure provides a PaaS network security, database, storage, and application services for Avail Technologies.

The applicable Trust Services Criteria that are intended to be met by controls at Azure, alone or in combination with controls at Avail Technologies, and the types of controls expected to be implemented at the Azure subservice organization to meet those Trust Services Criteria are described in the section below:

Control Activity Expected to be Implemented by Azure	Applicable Trust Services Criteria
Azure is responsible for restricting logical and physical access to and within the data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.8
Azure is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Azure is responsible for notifying Avail Technologies of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Control Activity Expected to be Implemented by Azure	Applicable Trust Services Criteria
Azure is responsible for the management of any third-party vendors with access to customer environments.	CC9.2
Azure is responsible for maintaining the availability of internet and power services, as well as preventative maintenance of cooling and power equipment.	A1.2
Azure is responsible for implementing controls to maintain confidentiality of information within the boundaries of the system.	C1.1

OneTrust

Avail Technologies uses OneTrust to provide continuous security and compliance monitoring. OneTrust provides resources to Avail Technologies to help meet various compliance requirements such as SOC 2 and other information security standards. OneTrust's read-only API gathers information for Avail Technologies' Management team and auditors and provides a dashboard to present the control data collected as well as display the overall adherence to the selected information security framework. OneTrust is responsible for the security of the OneTrust portal specific to Avail Technologies and limiting access to only those with business justification to the portal. OneTrust is also responsible for the security, confidentiality, and integrity of the information and data created, stored, or transferred via the client portal. OneTrust is also responsible for the processing integrity of their read-only API and for testing the completeness and accuracy of the API to validate it gathers and presents complete and accurate information to the client portal.

The applicable Trust Services Criteria that are intended to be met by controls at OneTrust, alone or in combination with controls at Avail Technologies, and the types of controls expected to be implemented at the OneTrust subservice organization to meet those Trust Services Criteria are described in the section below:

Control Activity Expected to be Implemented by OneTrust	Applicable Trust Services Criteria
OneTrust is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
OneTrust is responsible for the security, confidentiality, and integrity of the information and data created, stored or transferred via the client portal.	CC4.1, CC5.2, CC6.7
OneTrust is responsible for the security of the OneTrust portal specific to Avail Technologies and limiting access to only those with business justification to the portal.	CC6.1, CC6.2
OneTrust is responsible for encrypting client credentials at rest and restricting decryption access.	CC6.6, CC6.7
OneTrust is responsible for notifying Avail Technologies of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an Organization, and the way personnel conduct their activities, influencing how they carry out their control functions. This is the foundation for all other components of internal control, providing discipline and structure for business operations.

The control environment at Avail Technologies begins with Management's philosophy and operating style as well as the priorities and direction provided by the Executive Management Team. Avail Technologies' entire Organization is dedicated to delivering the highest level of customer service. The Company has created a corporate culture that supports this mission. The Company's Board of Directors is briefed by

Executive Management at least annually on the state of the Company's cybersecurity and privacy risk, as well as risks associated with security, availability, and confidentiality. The Board provides feedback and direction to Management as needed. Meeting minutes are documented and retained.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how they are communicated and how they are reinforced in practice. They include Management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

Avail Technologies has implemented, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. Avail Technologies' Management conducts business dealings with employees, suppliers, customers, investors, creditors, competitors, agents, resellers, counsel, accountants, regulators, and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes Management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Avail Technologies assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. Avail Technologies reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Organizational Structure

An entity's organizational structure provides the framework for how entity-wide objectives are planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and the nature of its activities.

The responsibilities of key positions within Avail Technologies are clearly defined and communicated to personnel. Individuals that hold key positions are knowledgeable and experienced within the industry. Avail Technologies' organizational structure supports the communication of information both up to leadership as well as down to support staff. Avail Technologies' organizational structure is comprised of ten primary business units that work together to deliver the Enterprise Transit Management Software System.

The ten business units consist of:

- ◇ Executive Management – Responsible for defining business objectives, information security, and operational procedures.
- ◇ Business Development – Responsible for branding and new client acquisition, customer support and fostering new business partnerships.
- ◇ Staff Engineers – Responsible for product development, data science, design, enhancement, and maintenance including customer retention and support.
- ◇ Products – Responsible for product implementation, customer retention, support, and other project management duties.
- ◇ Development, QA/Test, IT – Responsible for overseeing data management, creating data strategy, and improving data quality.
- ◇ Customer Experience – Responsible for creating, managing, and executing the customer experience strategy and priorities of the Company.

- ◇ Deployment Services – Responsible for planning, scheduling, and controlling the build, test and deployment of releases to deliver new or changed functionality, its enabling systems, technology and Organization while protecting the integrity of existing IT and Business Services.
- ◇ Programs – Responsible for managing, leading, and customizing new transport system solutions to the needs of each location.
- ◇ Finance and Operations – Responsible for overseeing all financial aspects of the business and driving the Company's financial strategy.
- ◇ Human Resources – Responsible for planning, leading, directing, developing, and coordinating the policies, activities, and staff, ensuring legal compliance and implementation of the Organization's mission and talent strategy.

HR Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and remedial action. Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate Avail Technologies' commitment to hiring and retaining only highly competent and trustworthy people. Personnel who work for Avail Technologies are required to read and acknowledge the Company's internal policies and confidentiality requirements as well as the confidentiality of customer-managed information.

Risk Assessment

Management is responsible for identifying the risks that threaten the achievement of the control objectives stated in its description of the Enterprise Transit Management Software System. Avail Technologies' Management has implemented a process for identifying relevant risks that occurs annually.

The risk assessment process consists of the following phases:

- ◇ Identifying – The identification phase includes documenting risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- ◇ Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- ◇ Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- ◇ Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- ◇ Monitoring – The monitoring phase includes the performance of monitoring activities by Avail Technologies' Management team to evaluate whether the processes, initiatives, functions and/or activities are mitigating the risk as designed.

In-Scope Trust Service Categories

The table below provides the TSCs within the scope of this report. The controls designed and implemented to meet the applicable TSC criteria are included in Section 4.

Trust Service Categories	Definition
Security	Information and systems are 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 entity's ability to achieve its objectives.
Availability	Information and systems are available for operation and use to meet the entity's objectives.
Confidentiality	Information designated as confidential is protected to meet the entity's objectives.

Security

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.

Availability

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The Availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with Management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws, regulations, contracts, or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the Privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Service Categories and Related Control Activities

Selection and Development of Control Activities

The applicable Trust Criteria and related control activities are included in the control matrices within Section 4 of this report, to eliminate the redundancy that would result from listing the items in this section. Although the control activities are included in the testing matrices set forth below in Section 4, they are, nevertheless, an integral part of Avail Technologies' description of its Enterprise Transit Management Software System. Any applicable Trust Services Criteria that are not addressed by control activities at Avail Technologies are also described within the control matrices.

Information and Communication

Information Systems

Avail Technologies, Inc.'s Enterprise Transit Management Software System is a SaaS platform running on Azure. Each client environment and data are separated based on the client's organization ID. Avail Technologies performs weekly full and daily incremental backups using Azure snapshots. Avail Technologies deploys TLS over HTTPS connections for migrating data from client systems to the Enterprise Transit Management Software System.

Communication

Information and communication are an integral component of Avail Technologies' internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity's operations.

Avail Technologies uses several information and communication channels internally to share information with Management, employees, contractors, and customers. Avail Technologies uses messaging systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Avail Technologies uses in-person and video weekly and monthly meetings to communicate Company priorities and goals.

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. Avail Technologies Management believes that open communication throughout the Organization ensures that deviations from standards are identified, reported, and appropriately addressed. External users are able to provide feedback and support requests via the "Connect with Us" link on the Company's website.

Monitoring

Monitoring is generally performed through active, hands-on management, including weekly Management meetings to discuss operational issues. Executive Management is involved and active in the business. Avail Technologies utilizes a risk-based approach to monitor business units and other auditable entities throughout the Organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

Management strives to be proactive in responding to customer complaints and maintain a high level of inter-departmental communication about these events. Customer complaints and other issues are handled via personal contact by Avail Technologies' Customer Support Team.

User Entity Controls

The control activities performed by Avail cover only a portion of the overall internal control structure of Avail Technologies' user organizations. Therefore, each customer's internal control structure must be evaluated in conjunction with Avail Technologies' control policies and procedures described in this report. Avail Technologies' controls over its Enterprise Transit Management Software System were designed with the understanding that certain user organization controls were in place and operating effectively.

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for maintaining their own system(s) of record.	CC2.1, A1.2
User entities are responsible for understanding and complying with their contractual obligations to Avail Technologies.	CC2.3
User entities are responsible for notifying Avail Technologies of changes made to technical or administrative contact information.	CC2.3
User entities are responsible for ensuring the supervision, management, and control of the use of services by Avail Technologies personnel including system access, roles, assignment of roles, and the monitoring of security access to Enterprise Transit Management Software System.	CC6.1
User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Enterprise Transit Management Software System.	CC7.2

User entities are responsible for immediately notifying Avail Technologies of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.	CC7.3
User entities are responsible for notifying Avail Technologies of any potential breaches of confidential information.	CC7.4, C1.1
User entities are responsible for using the secure methods provided by Avail Technologies to facilitate confidential data transfer.	C1.1
User entities are responsible for providing Avail Technologies data in accordance with their corporate confidentiality policies.	C1.1

Section 4: Trust Services Categories, Criteria, Related Controls, and Tests of Controls

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by Avail Technologies' Management throughout the examination period from April 1, 2024 to March 31, 2025. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved throughout the examination period. The nature of the tests conducted considered the type of control testing and the evidential matter available to perform a test to determine the operating effectiveness.

Types of Tests Performed:

- 1) **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the described control activity.
- 2) **Observation:** tests include the physical observation of the implementation, application of, or existence of specific controls.
- 3) **Inspection:** tests include the physical validation of documents, records, configuration, or settings.
- 4) **Re-performance:** tests include the reprocessing of transactions, procedures, and calculations to ensure the accuracy and completeness of the control description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by Avail Technologies:

Nature of Control and Frequency of Performance	Minimum Number of Items to Test
Occurrence based	10%, minimum of 5, maximum of 25
Manual control performed weekly	5
Manual control performed monthly	1
Manual control performed quarterly	1
Manual control performed annually	1
Application/Programmed control	Test one application of each programmed control for each type of transaction if supported by effective IT general controls (that have been tested); otherwise test at least 25

Trust Services Security, Criteria, Related Controls, and Tests of Controls

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC1.0	CONTROL ENVIRONMENT				
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	The Organization has defined and documented a Code of Conduct and Ethics and reviews them annually.	Inspected the Corporate Ethics Policy and revision history to verify that the Organization defined and documented a Code of Conduct and Ethics and reviewed them annually.	No exceptions noted.
		CC1.1.2	The Organization has established an Employee Handbook outlining requirements of the Code of Conduct, acceptable usage, and confidentiality commitments which are reviewed/updated on an annual basis by Executive Management. Employees are required to sign off on acceptance and acknowledgement of the Employee Handbook as part of the formal onboarding process and in the event of any significant revisions.	Inspected the Employee Handbook and acknowledgement for a sample of new hires to verify that the Organization established an Employee Handbook outlining requirements on the Code of Conduct, acceptable usage, and confidentiality commitments with employees required to sign off on acceptance and acknowledgment as part of the formal onboarding process. Inquired of the HR Representative I to verify that there were no significant revisions made to the Employee Handbook.	No exceptions noted.
		CC1.1.3	The Organization has established communication channels that allow employees to securely and, if needed, confidentially, report issues related to fraud, harassment, and other issues impacting the Organization's ethical and integrity requirements.	Inspected the Employee Handbook to verify that the Organization had established communication channels that allowed employees to report issues related to fraud, harassment, and other issues impacting the organization's ethical and integrity requirements. Inquired of the HR Representative I to verify that there were no code of conduct violations.	No exceptions noted.
		CC1.1.4	Third-party contractors working on behalf of the Organization are required to sign an agreement outlining Avail's standard code of conduct, security, and confidentiality requirements.	Inspected the signed independent contractor agreement for the only contractor onboarded to verify that contractors working on behalf of the Organization were required to sign contractual agreements.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC1.2	COSO Principle 2: The Board of Directors demonstrates independence from Management and exercises oversight of the development and performance of internal control.	CC1.2.1	The Board of Directors includes Non-Executive Directors that are independent from Management, and the Board meets on a quarterly basis for oversight on internal controls, operations, and business objectives.	Inspected the list of Board of Directors and meeting minutes for a sample of quarters to verify that the Board of Directors comprised of Non-Executive Directors independent from Management, and met quarterly to oversee internal controls, operations, and business objectives.	No exceptions noted.
		CC1.2.2	The Board of Directors' oversight responsibilities are defined and documented. The Board acknowledges to their responsibilities upon any changes.	Inspected the Avail Technologies, Inc. bylaws and the Board of Directors' acknowledgment of responsibilities to verify that the Board of Directors' oversight responsibilities were defined, documented, and acknowledged upon changes.	No exceptions noted.
		CC1.2.3	The Organization's Executive Team meets on a monthly basis to discuss operations, issues relating to internal controls, and delivery on key performance metrics.	Inspected the Security Committee meeting minutes for a sample of months to verify that the Organization's Executive Team met on a monthly basis to discuss operations, issues relating to internal controls, and delivery on key performance metrics.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications, and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	Inspected the job description and documented review for a sample of new hire positions to verify that job descriptions that documented the objectives of the role, responsibilities, reporting lines, employee qualifications, and other requirements were made available to employees and reviewed and updated annually or in the case of significant changes.	No exceptions noted.
		CC1.3.2	The Organization has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. The Organization structure is reviewed and updated in case of significant changes.	Inspected the organization chart to verify that the Organization had established an organizational chart defining roles, reporting lines, and authorities related to development, quality assurance, and security operations of its services, which was reviewed and updated in case of significant changes.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.1	The Organization utilizes OneTrust to manage its information security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policy and procedure documents are reviewed and approved by Management annually or during significant changes.	Inspected the Company's policy packet that was generated in OneTrust and its revision history to verify that the Organization utilized OneTrust to manage its Information Security policies and procedures, maintained internal policy and procedure documents related to security, confidentiality, and availability, and made them available to employees, and ensured they were reviewed and approved by Management annually or during significant changes.	No exceptions noted.
		CC1.4.2	Employees are required to complete an information security and awareness training class annually.	Inspected the information security and awareness training results dashboard for a sample of active employees to verify that employees were required to complete training annually.	No exceptions noted.
		CC1.4.3	The Organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	Inspected the completed performance evaluation for a sample of active employees to verify that the Organization had a process in place to evaluate the competency of employees and identify their development needs.	No exceptions noted.
		CC1.4.4	New employees are subjected to reference checks prior to joining the Organization.	Inspected the reference check for a sample of new hires to verify that new employees were subjected to reference checks prior to joining the Organization.	No exceptions noted.
		CC1.4.5	On an annual basis, Management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions, and applicable complementary user entity controls.	Inspected the attestation report and completed review for a sample of active vendors to verify that on an annual basis, Management performed reviews of SOC reports from service providers/vendors to assess the appropriateness of scope, impact of identified exceptions, and applicable complementary user entity controls.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results	
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.4.6	A vendor management process has been implemented whereby Management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	Inspected the attestation report and completed review for a sample of new vendors and active vendors to verify that a vendor management process was implemented whereby Management performed risk assessments of potential new vendors and evaluated the performance of existing vendors on an annual basis. Inquired of the Information Technology and Security Lead to verify that corrective actions were not required based on the assessments.	No exceptions noted.	
		CC1.3.1	See CC1.3.1.			
		CC1.5.1	The Organization uses OneTrust to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes, and policies is reviewed by Management on at least an annual basis and identified deficiencies are remediated in a timely manner.	Inspected the internal control assessment within OneTrust to verify that the Organization used OneTrust to document their internal controls and continuously monitor its effectiveness. Inquired of the Information Technology and Security Lead to verify that there were no deficiencies identified during the internal control review.	No exceptions noted.	
		CC1.1.2 CC1.1.3 CC1.4.3	See CC1.1.2, CC1.1.3, and CC1.4.3.			
CC2.0	COMMUNICATION AND INFORMATION					
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.1	Designated customer administrators and relevant organizational employees are trained on the functional use of the Transit Management application to understand their roles and responsibilities as part of the onboarding process.	Inspected the Training Plan for a sample of new customers to verify that designated customer administrators and relevant organizational employees were trained on the functional use of the Transit Management application to understand their roles and responsibilities as part of the onboarding process.	No exceptions noted.	

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.1.2	The Organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.	Inspected the Help Center on the Company's portal to verify that the Organization had developed documentation and user guides describing relevant system components, as well as the purpose and design of the system, which were made available and updated as needed.	No exceptions noted.
		CC1.5.1	See CC1.5.1.		
		CC2.2.1	Changes that affect the functionality and security of the system components are communicated to internal and external users.	Inspected the product updates and release notes page on the Company portal to verify that changes that affected the functionality and security of the system components were communicated to internal and external users.	No exceptions noted.
		CC2.2.2	A formal incident management process has been established and implemented which requires incidents to be tracked, documented, and resolved in a complete, accurate, and timely manner. The process document is reviewed by Management on an annual basis and updated as required.	Inspected the Incident Management Policy and the completed incident ticket for a sample of security incidents to verify that a formal incident management process had been established and implemented, requiring incidents to be tracked, documented, and resolved in a complete, accurate, and timely manner, with the process document reviewed annually by Management and updated as required.	No exceptions noted.
		CC1.1.2 CC1.1.3 CC1.1.4 CC1.2.1 CC1.2.3 CC1.4.1 CC1.4.2 CC2.1.2	See CC1.1.2, CC1.1.3, CC1.1.4, CC1.2.1, CC1.2.3, CC1.4.1, CC1.4.2, and CC2.1.2.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	The Organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenges through an appropriate channel. Reported incidents are addressed by the Organization's support staff in a timely manner.	Inspected the Help Center in the customer portal and a system-generated report of closed cases for a sample of customer support tickets to verify that the Organization provided an external-facing support system that allowed users to report incidents, complaints, issues, and other challenges through appropriate channels, which were addressed by the Organization's support staff in a timely manner.	No exceptions noted.
		CC2.3.2	The Organization has formal agreements in place with customers which acknowledges their compliance with security and confidentiality commitments.	Inspected the signed agreement for a sample of new customers to verify that the Organization had formal agreements in place with customers which acknowledged their compliance with security and confidentiality commitments.	No exceptions noted.
		CC2.3.3	New customer contracts or modifications to existing customer contracts and EULAs are reviewed annually by Management to ensure security and confidentiality commitments are met.	Inspected the signed agreement for a sample of new customers to verify that new customer contracts were reviewed annually by Management to ensure security and confidentiality commitments were met. Inquired of the Director of Customer Experience to verify that there no modifications made to existing customer contracts.	No exceptions noted.
		CC2.1.1 CC2.1.2	See CC2.1.1 and CC2.1.2.		
CC3.0	RISK ASSESSMENT				
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the Organization's Executive Management.	Inspected the completed risk assessment to verify that Management conducted a formal risk assessment annually, documenting and implementing identified risks and mitigation strategies with the involvement of the Organization's Executive Management.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC1.4.6 CC3.1.1	See CC1.4.6 and CC3.1.1.		
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.1.1	See CC3.1.1.		
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC1.4.6 CC3.1.1	See CC1.4.6 and CC3.1.1.		
CC4.0	MONITORING ACTIVITIES				
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.1	A penetration test is performed by an external vendor on an annual basis to identify security exploits. Issues identified are classified according to risk, and analyzed and remediated in a timely manner.	Inspected the penetration test to verify that a penetration test was performed annually to identify security exploits. Inquired of the Information Technology and Security Lead to verify that there were no critical or high-level findings that required remediation.	No exceptions noted.
		CC4.1.2	Internal and external vulnerability scanning is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	Inspected the Vulnerability Scanning Policy, vulnerability scanner dashboard results, and remediation documentation for a sample of quarters to verify that internal and external vulnerability scanning was performed on a quarterly basis to identify threats and vulnerabilities to the production systems, and any issues identified were analyzed and remediated in a timely manner.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
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.	CC1.2.3 CC1.4.5 CC1.5.1	See CC1.2.3, CC1.4.5, and CC1.5.1.		
		CC1.2.1 CC1.2.3 CC1.5.1	See CC1.2.1, CC1.2.3, and CC1.5.1.		
CC5.0	CONTROL ACTIVITIES				
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC1.2.3 CC1.5.1 CC3.1.1	See CC1.2.3, CC1.5.1, and CC3.1.1.		
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC1.5.1 CC3.1.1	See CC1.5.1 and CC3.1.1.		
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.	CC1.2.3 CC1.4.1 CC1.5.1	See CC1.2.3, CC1.4.1, and CC1.5.1.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC6.0	LOGICAL AND PHYSICAL SECURITY				
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.1	Unique user IDs and strong passwords are required in order to gain access to the infrastructure supporting the application (i.e. Active Directory, servers, and database accounts).	Inspected the Azure AD Password Policy and system-generated report of user IDs to verify that unique user IDs and strong passwords were required in order to gain access to the infrastructure supporting the application (i.e. Active Directory, servers, and database accounts).	No exceptions noted.
		CC6.1.2	Unique user IDs and strong passwords are required in order to gain access to the application production environment.	Inspected the application log-in page and password policy to verify that unique user IDs and strong passwords were required in order to gain access to the application production environment.	No exceptions noted.
		CC6.1.3	MFA is enforced for user accounts with administrative access to the Organization's production platform.	Inspected the Azure AD MFA Policy enforced to verify that MFA was enforced for user accounts with administrative access to the Organization's production platform.	No exceptions noted.
		CC6.1.4	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from Management prior to access provisioning.	Inspected the onboarding ticket for a sample of new hires to verify that access to in-scope system components required documented access request and approval from Management prior to access provisioning.	No exceptions noted.
		CC6.1.5	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees in a timely manner.	Inspected the separation ticket for a sample of terminated employees to verify that Management utilized an employee termination checklist to ensure that the termination process was consistently executed, and access was revoked for terminated employees.	No exceptions noted.
		CC6.1.6	System components are configured such that the Organization and its customers' access is appropriately segmented from other tenant users.	Inspected the system design diagram and a system-generated list of Azure VPCs and databases to verify that system components were configured such that the Organization and its customers' access was appropriately segmented from other tenant users.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
		CC6.1.7	The Organization maintains an inventory of production information assets including details on asset ownership, data classification, and location. The asset inventory listing is reviewed and updated by Management on an as-needed basis.	Inspected the asset inventory list to verify that the Organization maintained an inventory of production information assets, including details on asset ownership, data classification, and location, which was reviewed and updated by Management on an as-needed basis.	No exceptions noted.
		CC6.1.8	A formal network diagram outlining boundary protection mechanisms (e.g., firewalls) is maintained for all network connections and reviewed annually by IT Management.	Inspected the network diagram to verify that a formal network diagram outlining boundary protection mechanisms was maintained for all network connections, and was reviewed annually by IT Management.	No exceptions noted.
		CC6.1.9	The Organization uses its cloud provider Key Management Service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	Inspected the encryption report, encryption data columns, key rotation settings, and system-generated report of users with access to production keys to verify that the Organization used its cloud provider's Key Management Service to encrypt data at rest and manage encryption keys, while restricting access to production keys to authorized individuals.	No exceptions noted.
		CC6.1.10	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	Inspected the Key Management and Cryptography Policy and encryption settings for storage components to verify that customer data was encrypted at rest (stored and backup) using strong encryption technologies.	No exceptions noted.
		CC6.1.11	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	Inspected the results of the SSL server scan to verify that encryption technologies were used to protect communication and transmission of data over public networks and between systems.	No exceptions noted.
		CC6.1.12	Disk encryption and system passwords are enabled across Organization workstations.	Inspected the device encryption and password settings for a sample of active employee workstations to verify that disk encryption and system passwords were enabled across Organization workstations.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2.1	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	Inspected the completed user access review for a sample of quarters to verify that Management performed quarterly user access reviews for in-scope system components to ensure that access was restricted appropriately and modified or removed in a timely manner based on the results of the review.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.1.4 CC6.1.5	See CC6.1.4 and CC6.1.5.		
		CC6.3.1	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	<p>Inspected the system-generated list of users with privileged access to a sample of servers and databases to verify that access to a generic administrator or privileged accounts on the databases and servers supporting the application was restricted to authorized personnel based on a role-based access scheme.</p> <p>Inquired of the Information Technology and Security Lead to verify that access was restricted to authorized personnel based on a role-based access scheme.</p>	No exceptions noted.
		CC6.3.2	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	<p>Inspected the system-generated report of users with access to promote changes to production to verify that access to promote changes to production was restricted to authorized personnel based on job responsibilities.</p> <p>Inquired of the Director of Engineering to verify that users with access to promote changes to production was restricted to authorized personnel.</p>	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.1.4 CC6.1.5 CC6.2.1	See CC6.1.4, CC6.1.5, and CC6.2.1.		
		CC6.4.1	Physical security is the responsibility of Azure (refer to Section 3 for the subservice organization control activities).		
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data, and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	Formal data retention and disposal policies and procedures are in place to guide the secure retention and disposal of information.	Inspected the Data Retention and Disposal Policy, backup retention settings, and MDM remote wipe capabilities to verify that a formal data retention and disposal policy and procedure were in place to guide the secure retention and disposal of information. Inquired of the Project Manager to verify that there were no data disposal requests.	No exceptions noted.
		CC6.5.2	Data no longer required for its intended purpose is disposed of or destroyed in accordance with defined data retention and disposal procedures.	Inspected the Data Retention and Disposal Policy and MDM remote wipe capabilities to verify that data that was no longer required for its intended purpose was required to be disposed of or destroyed in accordance with procedures. Inquired of the Project Manager to verify that there were no data disposal requests.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.1	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols, and services. Firewall rules are reviewed on an annual basis by IT Management.	Inspected the Azure firewall rules report and documented review to verify that system firewalls were configured on the application gateway and production network to limit unnecessary ports, protocols, and services, and that firewall rules were reviewed annually by IT Management.	No exceptions noted.
		CC6.1.8 CC6.1.9 CC6.1.11	See CC6.1.8, CC6.1.9, and CC6.1.11.		
CC6.7		CC6.7.1	Production data is masked or anonymized when used outside of the production environment.	Inspected the data scrubbing and anonymization procedure, including a data export from the production database, customer data processing mapping, and a network diagram of the production environment to verify that production data was masked or anonymized when used outside of the production environment.	No exceptions noted.
	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.1.9 CC6.1.10 CC6.1.11 CC6.1.12	See CC6.1.9, CC6.1.10, CC6.1.11, and CC6.1.12.		
CC6.8		CC6.8.1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT Management on an annual basis and updated as needed.	Inspected the Software Change Management Procedure and review history to verify that a formal change management process existed, governing changes to the applications and supporting infrastructure, with the process document being reviewed by IT Management on an annual basis and updated as needed.	No exceptions noted.
		CC6.8.2	AV and anti-spam software is installed and enabled on servers to prevent or detect and act upon the introduction of unauthorized or malicious software.	Inspected the antivirus settings for a sample of production servers to verify that antivirus software was in place to prevent or detect and act upon the introduction of unauthorized or malicious software.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
		CC6.8.3	A centralized MDM solution has been deployed to mobile devices to enforce built-in detective and preventive security controls.	Inspected the MDM solution compliance status for a sample of active employee devices to verify that a centralized MDM solution was deployed to enforce built-in detective and preventive security controls on mobile devices.	No exceptions noted.
		CC6.8.4	Baseline configurations are retained within the configuration management tool for rollback capability if needed, when a configuration change is made.	Inspected the pipeline setup and configurations to verify that baseline configurations were retained within the configuration management tool for rollback capability if needed, when a configuration change was made.	No exceptions noted.
		CC6.8.5	Security software (firewall, AV, and anti-spam) is installed and enabled on workstations.	Inspected the security software agents installed on a sample of active employees' workstations to verify that security software (firewall, anti-virus, and anti-spam) was installed and enabled on workstations.	No exceptions noted.
		CC6.3.1	See CC6.3.1.		
CC7.0	SYSTEM OPERATIONS				
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.1	A log management system and process has been formalized ensure that access to change the log configuration and access to modify logs is restricted.	Inspected the Log Management Process Guide, a report of users with access to logs, and the documented approval of those users to verify that a log management system and process were formalized to ensure that access to change the log configuration and modify logs was restricted.	No exceptions noted.
		CC7.1.2	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT Management, and issues identified are resolved in a timely manner through the incident management process.	Inspected the system-generated event log, alert rules, action groups, monitoring examples, and recent alert to verify that logging was enabled to monitor various activities, with automated alerts configured to notify IT Management. Inquired of the IT Manager to verify that there were no issues identified that initiated the incident management process.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
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.	CC4.1.1 CC4.1.2 CC6.8.4	See CC4.1.1, CC4.1.2, and CC6.8.4.		
		CC7.2.1	Incidents related to security are logged, tracked, and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.	Inspected the Incident Management Policy and completed incident ticket for a sample of security incidents to verify that incidents related to security were logged, tracked, and communicated to affected parties, and were resolved in a timely manner in accordance with the formal incident management process.	No exceptions noted.
		CC7.2.2	The IT Team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. The incident management process is invoked for confirmed events and anomalies.	Inspected the monitoring metrics, alert thresholds, and alert recipients to verify that the IT Team continuously monitored system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Inquired of the IT Manager to verify that there were no events or anomalies identified that initiated the incident management process.	No exceptions noted.
		CC2.2.2 CC6.6.1 CC7.1.2	See CC2.2.2, CC6.6.1, and CC7.1.2.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.1	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the Organization's privacy and confidentiality commitments.	Inspected the Incident Management Policy to verify that notifications regarding confirmed data breaches were to be provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments. Inquired of the IT Manager to verify that there were no data breaches reported.	Non-Occurrence noted. Pease Bell was unable to opine on the operating effectiveness of this control activity as there were no confirmed data breaches reported during the examination period.
		CC7.3.2	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	Inspected the post-incident review for a sample of security incidents to verify that Management incorporated lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	No exceptions noted.
		CC2.2.2 CC7.2.1	See CC2.2.2 and CC7.2.1.		
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC7.4.1	Daily full-system backups are performed using an automated system that replicates the backups to an offsite location. Backups are monitored for failure using an automated system.	Inspected the backup schedule, replication settings, and backup report summary to verify that daily full-system backups were performed using an automated system that replicated the backups to an offsite location, with failures monitored by the automated system.	No exceptions noted.
		CC7.4.2	Disaster recovery plans (including restoration of backups) have been developed and are tested annually. Test results are reviewed, and consequently contingency plans are updated.	Inspected the Disaster Recovery Plan and the Disaster Recovery Test Results to verify that disaster recovery plans, including restoration of backups, were developed and tested annually, with the test results reviewed and contingency plans updated accordingly.	No exceptions noted.
		CC7.4.3	Management has established defined roles and responsibilities to oversee the implementation of security policies including incident response.	Inspected the Incident Management Policy to verify that Management had established defined roles and responsibilities for overseeing the implementation of security policies, including incident response.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC2.2.2 CC2.3.1 CC4.1.2 CC7.2.1 CC7.3.1 CC7.3.2	See CC2.2.2, CC2.3.1, CC4.1.2, CC7.2.1, CC7.3.1, and CC7.3.2.		
		CC7.5.1	A patch management process exists to confirm that operating system level vulnerabilities for servers are remediated in a timely manner. In addition, production servers are scanned to test patch compliance on a quarterly basis.	Inspected the system generated exports of servers with the patch management solution installed, and patching schedule for a sample of quarters to verify that a patch management process existed to confirm that operating system-level vulnerabilities for servers were remediated in a timely manner, and production servers were scanned to test patch compliance on a quarterly basis.	No exceptions noted.
		CC7.5.2	A patch management process exists to confirm that operating system level vulnerabilities for workstations are remediated in a timely manner and scanned for compliance on a continuous basis.	Inspected the Workstation Security Policy and patch manager update and scan settings to verify that a patch management process existed to confirm that operating system level vulnerabilities for workstations would have been remediated in a timely manner and scanned for compliance on a continuous basis.	No exceptions noted.
		CC7.2.1 CC7.3.2	See CC7.2.1 and CC7.3.2.		
CC8.0	CHANGE MANAGEMENT				
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC8.1.1	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.	Inspected the completed change ticket for a sample of emergency changes to verify that emergency change requests were documented and subjected to the standard change management process but at an accelerated timeline, with appropriate approval obtained and documented prior to initiating an emergency change.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
		CC8.1.2	A formal SDLC methodology is established that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.	Inspected the Software Development Policy and change flow diagram to verify that a formal SDLC methodology was established that governed the development, acquisition, implementation, and maintenance of application development and enhancement projects.	No exceptions noted.
		CC8.1.3	Changes to the application(s) and supporting infrastructure are documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	Inspected the Software Change Management Procedure and completed ticket for a sample of infrastructure/application changes to verify that changes to the application(s) and supporting infrastructure were documented, tested, and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	No exceptions noted.
		CC8.1.4	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.	Inspected the system infrastructure environment pipelines to verify that changes to application and system infrastructure were developed and tested in a separate development or test environment before implementation.	No exceptions noted.
		CC2.2.1 CC6.3.2 CC6.7.1 CC6.8.1 CC6.8.4	See CC2.2.1, CC6.3.2, CC6.7.1, CC6.8.1, and CC6.8.4.		
CC9.0	RISK MITIGATION				
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.1	Management maintains insurance coverage through an external service provider against major financial risks for the overall business, including cyber risks.	Inspected the insurance policy coverage to verify that Management maintained insurance coverage through an external service provider against major financial risks for the overall business, including cyber risks.	No exceptions noted.
		CC3.1.1	See CC3.1.1.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	A vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.	Inspected the Vendor Management Policy to verify that a vendor management process had been in place that included security procedures to be followed in case of vendor terminations. Inquired of the Director of Technology to verify that there were no vendor terminations.	Non-Occurrence noted. Pease Bell was unable to opine on the operating effectiveness of this control activity as there were no confirmed vendor terminations during the examination period.
		CC1.4.5 CC1.4.6	See CC1.4.5 and CC1.4.6.		
A1.0	ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	CC7.2.2	See CC7.2.2.		
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.	CC7.4.1 CC7.4.2	See CC7.4.1 and CC7.4.2.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Tests of Operating Effectiveness	Test Results
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CC7.4.2	See CC7.4.2.		
C1.0	ADDITIONAL CRITERIA FOR CONFIDENTIALITY				
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C1.1.1	The Organization has formalized data classification policies and procedures to identify confidential information in the system and to define instructions for handling and labelling confidential information.	Inspected the Information Classification Policy and a classified document to verify that the Organization formalized data classification policies and procedures to identify confidential information in the system and to define instructions for handling and labeling confidential information.	No exceptions noted.
		CC6.1.6 CC6.5.1 CC6.7.1	See CC6.1.6, CC6.5.1, and CC6.7.1.		
C1.2		CC6.5.1 CC6.5.2	See CC6.5.1 and CC6.5.2.		