

SOC 2 Type 2 Report

TRANSFUSION ANTIBODY EXCHANGE, Inc.



August 28, 2023 to February 27, 2024

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY



Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

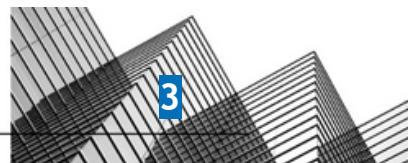
www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

AICPA NOTICE:

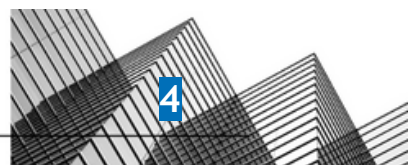
You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

Table of Contents

Management's Assertion	6
Independent Service Auditor's Report	9
Scope	9
Service Organization's Responsibilities	9
Service Auditors' Responsibilities	10
Inherent Limitations	11
Opinion	11
Restricted Use	11
System Description	13
DC 1: Company overview and types of products and services provided.	14
DC 2: The principal service commitments and system requirements.	14
DC 3: The components of the system used to provide the services.	15
3.1 Primary Infrastructure:	15
3.2 Primary Software:	15
3.3 People:	16
3.4 Security Processes and Procedures:	16
3.5 Data:	17
3.6 Third Party Access:	17
3.7 System Boundaries: (Product lines/ LOBs/ brands)	17
DC 4: Disclosures about identified security incidents.	18
DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.	18
5.1 Integrity and Ethical Values	18
5.2 Commitment to Competence	18
5.3 Management's Philosophy and Operating Style (Culture of the company/ Leadership style/ website)	18
5.4 Organizational Structure and Assignment of Authority and Responsibility (Job description and org chart/ HR policy)	18
5.5 Human Resource Policies and Practices	19
5.6 Security Management	19
5.7 Security and Privacy Policies	19
5.8 Personnel Security	19
5.9 Physical Security and Environmental Controls	19
5.10 Change Management	20
5.11 System Monitoring	20
5.12 Incident Management	20
5.13 Data Backup and Recovery	20
5.14 System Account Management	20



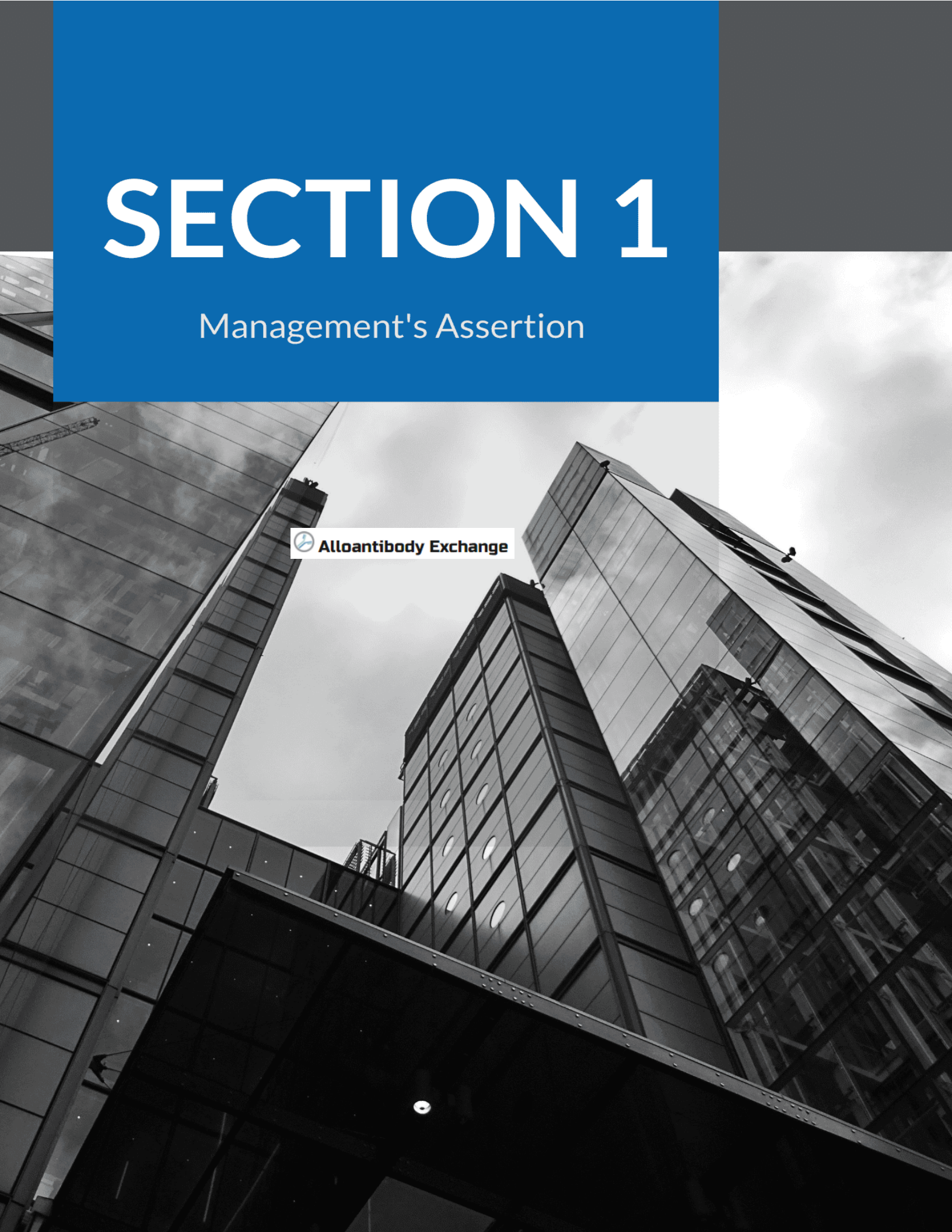
5.15 Data Classification	20
5.16 Risk Management Responsibilities	21
5.17 Risk Management Program Activities	21
5.18 Integration with Risk Assessment	21
5.19 Information and Communications Systems	21
5.20 Data Communication	21
5.21 Monitoring Controls	22
DC 6: Complementary User Entity Controls (CUECs):	22
DC 7: Complementary Subservice Organization Controls (CSOCs):	22
DC 8: Disclosures of out-of-scope Trust Services Criteria	23
DC 9: Disclosures of significant changes in last 1 year	23
Testing Matrices	24
Tests of Operating Effectiveness and Results of Tests	25
Scope of Testing	25
Types of Tests Generally Performed	25
General Sampling Methodology	26
Reliability of Information Provided by the Service Organization	27
Test Results	27



SECTION 1

Management's Assertion

 Alloantibody Exchange



Management's Assertion

We have prepared the accompanying description of TRANSFUSION ANTIBODY EXCHANGE's system throughout the period August 28, 2023 to February 27, 2024, 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. The description is intended to provide report users with information about TRANSFUSION ANTIBODY EXCHANGE's system that may be useful when assessing the risks arising from interactions with TRANSFUSION ANTIBODY EXCHANGE's system, particularly information about system controls that TRANSFUSION ANTIBODY EXCHANGE 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 set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

- a. The description presents TRANSFUSION ANTIBODY EXCHANGE's system that was designed and implemented throughout the period August 28, 2023 to February 27, 2024 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period August 28, 2023 to February 27, 2024, to provide reasonable assurance that TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of TRANSFUSION ANTIBODY EXCHANGE's controls during that period.
- c. The controls stated in the description operated effectively throughout the period August 28, 2023 to February 27, 2024 to provide reasonable assurance that TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of TRANSFUSION ANTIBODY EXCHANGE's controls operated effectively throughout the period.

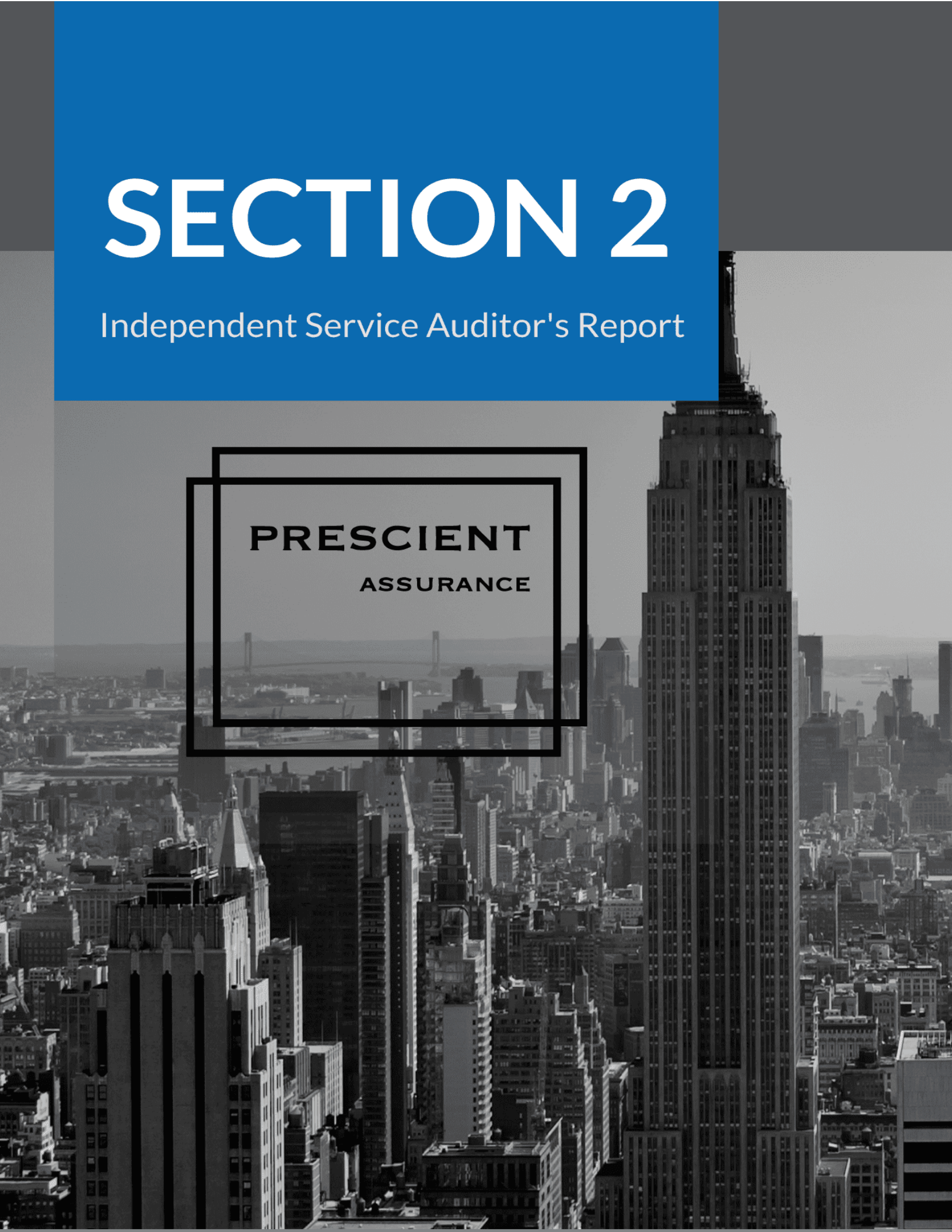
Ronald "George" Hauser, MD
President
TRANSFUSION ANTIBODY EXCHANGE, Inc.



SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE



Independent Service Auditor's Report

To: TRANSFUSION ANTIBODY EXCHANGE

Scope

We have examined TRANSFUSION ANTIBODY EXCHANGE's ("TRANSFUSION ANTIBODY EXCHANGE") accompanying description of its Alloantibody Exchange system found in Section 3, titled TRANSFUSION ANTIBODY EXCHANGE System Description throughout the period August 28, 2023 to February 27, 2024 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, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 28, 2023 to February 27, 2024 to provide reasonable assurance that TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

TRANSFUSION ANTIBODY EXCHANGE uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TRANSFUSION ANTIBODY EXCHANGE, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents TRANSFUSION ANTIBODY EXCHANGE's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TRANSFUSION ANTIBODY EXCHANGE's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

TRANSFUSION ANTIBODY EXCHANGE 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 TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements were achieved. In Section 1, TRANSFUSION ANTIBODY EXCHANGE has provided the accompanying assertion titled "Management's Assertion of TRANSFUSION ANTIBODY EXCHANGE" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. TRANSFUSION ANTIBODY EXCHANGE 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 Auditors' 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 operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. 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.
6. 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 individual report users may consider important to

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

Opinion

In our opinion, in all material respects:

- a. The description presents TRANSFUSION ANTIBODY EXCHANGE's system that was designed and implemented throughout the period August 28, 2023 to February 27, 2024 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period August 28, 2023 to February 27, 2024 to provide reasonable assurance that TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of TRANSFUSION ANTIBODY EXCHANGE's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period August 28, 2023 to February 27, 2024 to provide reasonable assurance that TRANSFUSION ANTIBODY EXCHANGE's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of TRANSFUSION ANTIBODY EXCHANGE's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of TRANSFUSION ANTIBODY EXCHANGE, user entities of TRANSFUSION ANTIBODY EXCHANGE's system during some or all of the period August 28, 2023 to February 27, 2024, business partners of TRANSFUSION ANTIBODY EXCHANGE 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:

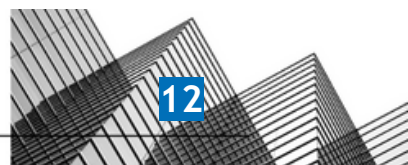
1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Prescient Assurance LLC

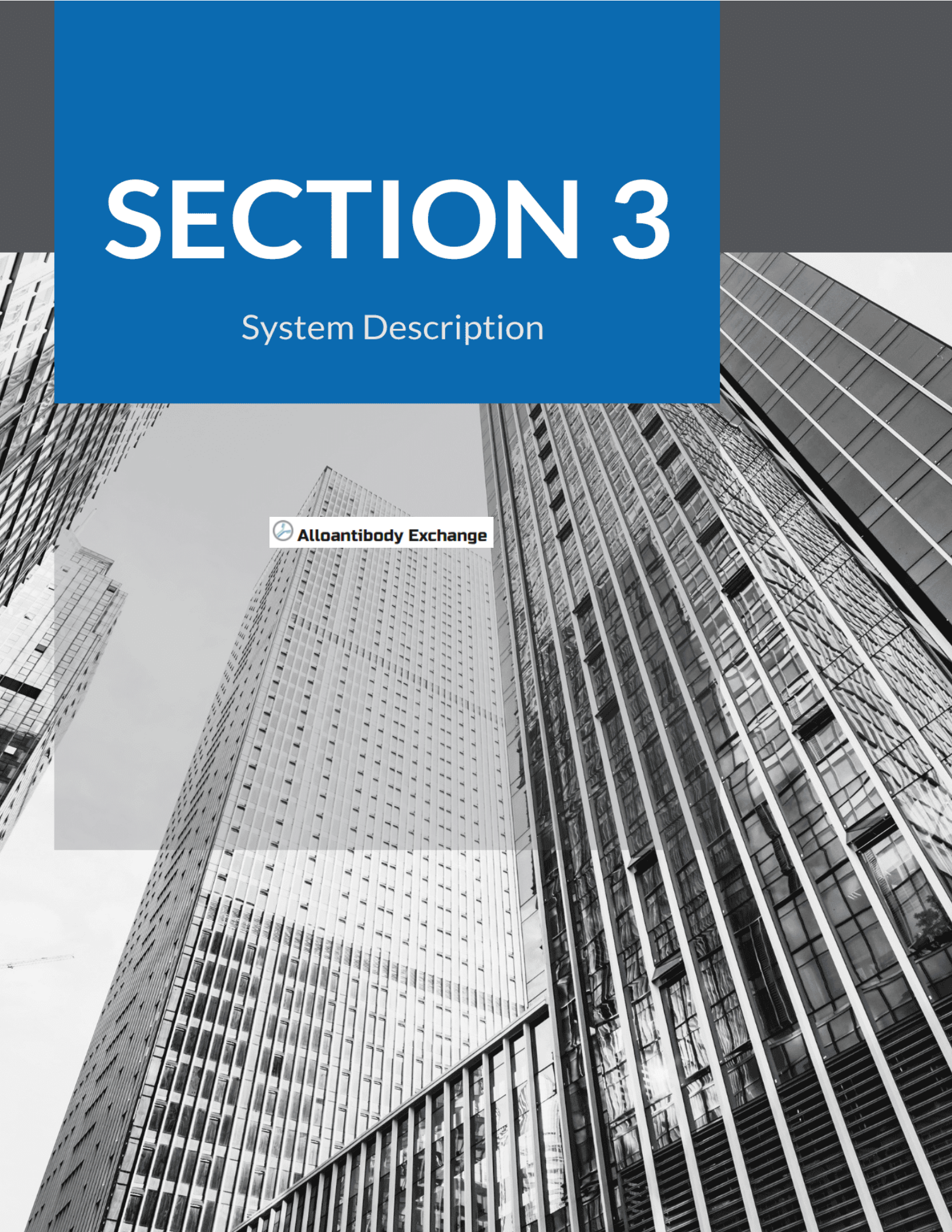
John D. Wallace, CPA
Chattanooga, TN
May xx, 2024



SECTION 3

System Description

 **Alloantibody Exchange**



DC 1: Company overview and types of products and services provided.

The Transfusion Antibody Exchange provides a service, the Alloantibody Exchange. The Alloantibody Exchange enables those who provision blood products to review a more complete patient transfusion history, which provides numerous benefits including the prevention of delayed hemolytic transfusion reactions in transfusion recipients.

Issues associated with an incomplete patient transfusion history are well known in the field of transfusion medicine. Blood bank accreditation organizations (e.g., AABB, CAP, Joint Commission) uniformly require the review of a patient's transfusion history prior to transfusion. The implementation of this requirement is variable, but generally, the review is limited to information readily available in the host system. Many blood banks phone other local blood banks with their inquiry, an insecure, slow, and incomplete, but necessary, process. Health systems may contain more than one blood bank, and they frequently lack the ability to electronically exchange information between themselves, even for patients seen within their health system. Over a dozen peer reviewed academic research papers have advocated for the adoption of a system like the Alloantibody Exchange, documenting its cost-effectiveness and, in the largest study of its kind, a reduction in the occurrence of delayed hemolytic transfusion reactions by 50%.

The Transfusion Antibody Exchange is a 501(c)(3) non-profit. It was formed by a coalition of like minded transfusion medicine physicians and informatics experts to improve the safety of transfusion. It is the recipient of grants from Microsoft, Google, and Abbott. The AABB has awarded its supporters the President's Award.

DC 2: The principal service commitments and system requirements.

Transfusion Antibody Exchange makes service commitments to its customers. It is responsible for these service commitments and for designing, implementing, and operating effective controls with the Alloantibody Exchange to provide reasonable assurance that Transfusion Antibody Exchange's service commitments are achieved.

Service commitments to customers are documented in the Alloantibody Exchange service agreement. These include, but are not limited to, the following:

- Security: Transfusion Antibody Exchange has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including many modern security features including end-to-end encryption, Microsoft Entra Id (formerly Azure Active Directory), role memberships, object-level authorizations, IP firewalls, requirements for application registration, SQL database auditing, and geo-redundant backup storage.

DC 3: The components of the system used to provide the services.

3.1 Primary Infrastructure:

Transfusion Antibody Exchange utilizes the Microsoft Azure Cloud to host the Alloantibody Exchange. Primary resources include:

- Microsoft Azure Web Application
- Microsoft SQL Server Database
- Microsoft Azure Entra Id (formerly Azure Active Directory)
- Microsoft Log Analytics Workspace
- Microsoft Defender for Cloud

Figure. Microsoft Azure Entra Id (formerly Active Directory) provides authentication and authorization to endpoints (2.) and (3.).

1. Public access (e.g., alloantibody.org)
2. Health system retrieval of a patient's transfusion history.
3. Health system upload of patients' transfusion histories. This is a REST API.

3.2 Primary Software:

The Alloantibody Exchange consists of two software components:

- Alloantibody Exchange Web Application
 - The web application facilitates the submission and retrieval of patient's transfusion histories.
 - The web application supports the implementation process by providing a visual display of the project plan and a list of stakeholders.
- Alloantibody Exchange ETL Application
 - The ETL application is used by health systems to submit their patient's transfusion histories.
 - The health system may choose to use other means to send their data. This is one such option.

Primary Software

System/Application	Operating System	Purpose
Alloantibody Exchange Web Application	N/A	<ul style="list-style-type: none">● The web application facilitates the submission and retrieval of patient's transfusion histories.● The web application supports the implementation process by providing a visual display of the project plan and a list of stakeholders.

Alloantibody
Exchange ETL
Application

Windows (e.g.,
Windows Server
2022)

- The ETL application is used by health systems to submit their patient's transfusion histories.
- The health system may choose to use other means to send their data. This is one such option.

3.3 People:

The Transfusion Antibody Exchange includes the following key roles with respect to data security:

- **Board of Directors:** Provides oversight and guidance to senior management.
- **Senior Management:** Converts the mission of the Transfusion Antibody Exchange into actionable steps to realize our goal of improving the safety of blood transfusion. They receive guidance from the Board of Directors.
- **Information Security Officer:** Operates the information security program including effective risk management. Their role includes identifying risks, threats, and vulnerability. It also includes adding controls to mitigate these risks.

3.4 Security Processes and Procedures:

We update, maintain, and adhere to the following data security policies:

- Acceptable Use Policy
- Access Control and Termination Policy
- Board of Directors Policy
- Bring Your Own Device Policy
- Business Continuity and Disaster Recovery Plan Policy
- Change Management Policy
- Code of Conduct Policy
- Confidentiality Agreement Policy
- Configuration and Asset Management Policy
- Data Classification Policy
- Data Retention and Disposal Policy
- Encryption and Key Management Policy
- Information Security Policy
- Network Security Policy
- Organizational Chart Policy
- Performance Review Policy
- Physical Security Policy
- Risk Assessment and Treatment Policy
- Roles and Responsibilities Policy
- Secure Development Policy
- Security Incident Response Plan Policy
- Vendor Management Policy

- Vulnerability and Patch Management Policy

In addition, we provide the following documents to customers related to data security:

- Alloantibody Exchange HIPAA
- Alloantibody Exchange OWASP - Web application

3.5 Data:

Overview

The data flows from the health systems to our cloud and back to the health systems. This allows the health system's blood banks to share patient transfusion histories.

Figure. Artistic rendition of data packets flowing from a health system to the Alloantibody Exchange. The Alloantibody Exchange sends individual patient transfusion histories back to the health system upon request.

Data Flow from the Health System to the Alloantibody Exchange

Figure. The Alloantibody Exchange ETL Application (middle) submits blood bank data from the site (left) to the Alloantibody Exchange Cloud (right).

- [Left] The blood bank database will vary by vendor (e.g., Cerner uses Oracle. WellSky uses Microsoft). It may not be the same vendor as the EHR (e.g., Epic).
- [Middle] The health system will host the Alloantibody Exchange ETL Application within a Windows environment. (For healthcare systems with a Microsoft Enterprise license, there is no cost with setting up a Windows VM.) The Alloantibody Exchange will provide the application, which runs once daily during off hours.
- [Right] The REST API uses HTTPS encryption (port 443) with OpenID Connect (authentication) / OAuth2.0 (authorization).

Data Flow from the Alloantibody Exchange to the Health System

Figure. Users access the Alloantibody Exchange web portal to retrieve patient information.

3.6 Third Party Access:

The Alloantibody Exchange does not allow third party access.

3.7 System Boundaries: (Product lines/ LOBs/ brands)

The Alloantibody Exchange operates as a distinct product.

DC 4: Disclosures about identified security incidents.

The Alloantibody Exchange has experienced no significant system incidents in its history that either (a) resulted in a significant failure in the achievement of one or more of its service commitments and system requirements or (b) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements.

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

5.1 Integrity and Ethical Values

Our nonprofit is committed to executing our mission with integrity and adherence to ethical values. Personnel must adhere to a Code of Conduct Policy and Confidentiality Agreement as a condition of employment. Our work has multiple levels of oversight including an independent Board of Directors.

5.2 Commitment to Competence

Personnel must demonstrate competence through multiple mechanisms. Personnel undergo a background check, perform security training, and understand/acknowledge our policy manual as part of hiring and training. Personnel receive an annual performance review. These tasks are outlined in multiple policies: Information Security Policy and the Roles and Responsibilities Policy.

5.3 Management's Philosophy and Operating Style (Culture of the company/ Leadership style/ website)

The Transfusion Antibody Exchange management philosophy prioritizes fairness, equity, and respect. This operating style is codified in our Code of Conduct.

5.4 Organizational Structure and Assignment of Authority and Responsibility (Job description and org chart/ HR policy)

Our organization contains a Board of Directors that oversee the operation of the nonprofit by management. The Board of Directors Policy outlines the principles that govern the Board of Directors including the charter, scope, and membership. The Roles and Responsibilities Policy contain written descriptions in the duties of management.

5.5 Human Resource Policies and Practices

Multiple policies govern our human resources. For example, the Code of Conduct Policy defines the expected behavior from employees or volunteers. The Acceptable Use Policy outlines the acceptable use of software and data systems. Finally, the Access control and Termination Policy details the onboarding and offboarding of personnel.

5.6 Security Management

The Roles and Responsibilities Policy contains details on how we manage information security. It contains the roles and responsibilities attributed to specific jobs. It applies to all employees, providing them with a job description, expectations, roles, and responsibilities.

5.7 Security and Privacy Policies

Our Security and Privacy practices are detailed in multiple policies. These policies include:

- Information Security Policy
- Access Control and Termination Policy
- Bring Your Own Device Policy
- Change Management Policy
- Configuration and Asset Management Policy
- Data Classification Policy
- Data Retention and Disposal Policy
- Encryption and Key Management Policy
- Network Security Policy
- Physical Security Policy
- Secure Development Policy
- Vulnerability and Patch Management Policy

In addition to these policies, we perform an annual HIPAA security review. We also perform the Security Risk Assessment Tool sponsored by the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR).

5.8 Personnel Security

Our policies require our personnel to meet multiple criteria before participating in activities related to the Alloantibody Exchange. For example, employees have a background check performed, perform security training, agree to a Code of Conduct, and understand/acknowledge our policy manual.

5.9 Physical Security and Environmental Controls

The Transfusion Antibody Exchange operates as a remote company without a centralized headquarters or physical network. The physical and environmental security for our data operations are overseen by our cloud provider, Microsoft. Specific considerations of physical security with remote work are found in our Bring Your Own Device Policy.

5.10 Change Management

Our Change Management Policy outlines the process for executing change within our organization, particularly with respect to software. The policy outlines the goal of software change to include (1) the minimization of service disruptions associated with change implementation and (2) to ensure stability and performance. It details the process of change from change identification through design, documentation, and tracking, change testing, approval, notification, deployment, and finally validation. It identifies the individuals responsible for these actions along with how the process is monitored and reviewed.

5.11 System Monitoring

We employ a suite of tools to monitor our systems. Examples include the utilization of Microsoft Defender for Cloud in our Information Security Policy, multifactor authentication in our Access Control and Termination Policy, and the review of database, source code, and active directory audit logs.

5.12 Incident Management

We have a Security Incident Response Plan Policy. It details the deployment of an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches through Microsoft Defender for Cloud. The intrusion detection system has email alerting enabled. It also includes an Incident Response and Breach Notification Plan, which involves our Computer Security Incident Response Team (CSIRT). CSIRT team members and responsibilities are detailed in this plan. We regularly test our CSIRT team with Security Incident Response Tests.

5.13 Data Backup and Recovery

We have a Business Continuity and Disaster Recovery Plan Policy. The policies outline the identification, communication, incident response, and recovery strategy. A specific section titled, Data and Systems Backup, provides step-by-step instructions to restore company data from a backup. A Disaster Recovery Plan Test is routinely performed to ensure familiarity with the procedure.

5.14 System Account Management

Our Access Control and Termination Policy outlines the principles governing access to company systems and data as well as the process of removing that access upon termination. This policy puts into place systems to protect sensitive information, ensure data integrity, and ensure system reliability. It includes details on identification/authentication and authorization. Authorization includes providing permissions to data sources and organizing those data sources according to our data classification policy. Instructions for the onboarding and offboarding of employees is detailed in the Access Control and Termination Policy.

5.15 Data Classification

We have a Data Classification Policy. It describes the three classes of data we manage: critical, private, and unrestricted. Critical data include any PHI, audit logs, and system credentials. Private data includes internal communications and source code. Unrestricted data includes data available for

display on the web, which may include letters of support for the project. Access to each class of data is managed according to our Roles and Responsibilities Policy.

5.16 Risk Management Responsibilities

We actively maintain a Risk Assessment and Treatment Policy. It includes a risk identification over various classes of threats including:

- Theft, fraud, extortion, embezzlement
- Elevated privileges, unacceptable use, password mishandling
- Network security issues, source code security issues, improper data sharing
- Viruses, ransomware code injection, DDOS attacks, phishing

The Risk Assessment and Treatment Policy has details on the analysis and mitigation of these risks including assignment to individuals or teams responsible for implementation of safeguards and risk-mitigating controls.

5.17 Risk Management Program Activities

Our Risk Assessment and Treatment Policy details the identification, evaluation, treatment, and monitoring of risks. An additional policy, Security Incident Response Plan, has details on incidence response, breach notification, and our Computer Security Incident Response Team (CSIRT). Further risk management is contained in the Business Continuity and Disaster Recovery Plan Policy.

5.18 Integration with Risk Assessment

We integrate multiple factors into the assessment of risk spanning business and information security risks. Relevant policies for a holistic view of risk include our Board of Directors Policy (e.g., oversight of theft, fraud), Access Control and Termination Policy (e.g., access management), Network Security Policy, and Information Security Policy (e.g., protection from viruses).

5.19 Information and Communications Systems

Our Information Security Policy details the security of our information and communications systems. For example, we employ Microsoft Defender for Cloud, GitHub's Dependabot security vulnerability detector, and log management tools (e.g., SQL Server database logs, Azure active directory logs, and GitHub commit logs). We have password requirements and lockout criteria for failed logins. Additional details are covered in our Encryption and Key Management Policy.

5.20 Data Communication

We maintain an Encryption and Key Management Policy. The policy outlines the procedures regarding encryption of data, communications, and encryption or access keys. It applies to data held by us, communicated with us, and to any documents or other data stores within our purview that may contain protected information.

5.21 Monitoring Controls

To monitor the controls we have established, we maintain a schedule of tasks documented in our Policy Review and Control Action Frequency. The schedule is divided into annual, quarterly, and monthly tasks. Examples of annual tasks include our risk assessment, Board of Directors annual report, employee performance review, and security awareness training. Examples of quarterly tasks include the review of access privileges, and the board of directors update meeting. Monthly tasks include review of vulnerability scans and audit logs. We also perform maintenance as dictated by work or on a continuous basis including software code changes and testing.

DC 6: Complementary User Entity Controls (CUECs):

There are no controls at the user entity that are necessary, in combination with Transfusion Antibody Exchange's controls, to provide reasonable assurance that Transfusion Antibody Exchange's service commitments and system requirements were achieved based on the applicable trust services criteria.

There are, however, certain responsibilities that users of the Alloantibody Exchange should fulfill for the user entity to derive the intended benefits.

Example User Entity Responsibility	
Criteria	Complementary Subservice Organization Controls
CC2.1	User entities ensure the quality of the information it generates and shares with the Alloantibody Exchange.
CC6.4	User entities are required to restrict access to the Alloantibody Exchange to authorized personnel.

DC 7: Complementary Subservice Organization Controls (CSOCs):

This description does not extend to the services provided by Microsoft's Azure Cloud on which Alloantibody Exchange depends. Section 4 of this report and this description of the system only cover the relevant trust services criteria and related controls in support of the achievement of Transfusion Antibody Exchange's service commitments and system requirements. It excludes the controls fulfilled by Microsoft's Azure Cloud (see Table).

Example Trust Criteria Performed by Microsoft's Azure Cloud

Criteria	Complementary Subservice Organization Controls
CC6.4	Microsoft Azure is responsible for restricting data center access to authorized personnel.
CC6.4	Microsoft Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	Microsoft Azure is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	Microsoft Azure is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	Microsoft Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.

Microsoft provides System and Organization Controls (SOC) reports for the Azure Cloud online.

DC 8: Disclosures of out-of-scope Trust Services Criteria

There were no specific security Trust Services Criteria as set forth in TSP Section 100 that were not relevant to the system as presented in this report.

DC 9: Disclosures of significant changes in last 1 year

The Alloantibody Exchange has not undergone significant changes in the last year.

SECTION 4

Testing Matrices

**PRESCIENT
ASSURANCE**

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Alloantibody Exchange provided by TRANSFUSION ANTIBODY EXCHANGE. The scope of the testing was restricted to Alloantibody Exchange, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period August 28, 2023 to February 27, 2024.

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: <ul style="list-style-type: none">• Examination / Inspection of source documentation and authorizations to verify transactions processed.• Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.• Examination / Inspection of systems documentation, configurations, and settings; and• Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.



Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2



Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

Reliability of Information Provided by the Service Organization

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.



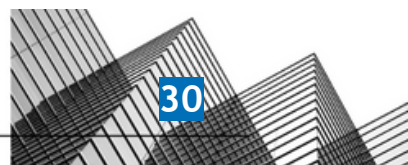
Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees in accordance with local laws.	<p>Inquired of the President on May 2, 2024 regarding background checks to determine that no personnel were onboarded during the audit window.</p> <p>Inspected the Information Security Policy to determine that the company performs background checks on new employees in accordance with local laws.</p> <p>Inspected the onboarding document to determine that no onboarding events took place during the audit period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Not tested, did not occur during observation.</p>
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	<p>Inquired of the President on May 2, 2024 to determine that no contractors were onboarded during the audit window.</p> <p>Inspected the Information Security Policy to determine that the company requires contractor agreements to include a code of conduct or reference to the company code of conduct.</p> <p>Inspected onboarding documentation to determine that there are no contractors employed by the company.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Not tested, did not occur during observation.</p>
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	<p>Inquired of the President on May 2, 2024 to determine that no employees were on-boarded during the audit window.</p> <p>Inspected the Information Security Policy to determine that the company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.</p> <p>Inspected onboarding documentation to determine that there were no employees onboarded during the audit window.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Not tested, did not occur during observation.</p>
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires all employees and full-time contractors to sign an industry	Inquired of the President on May 2, 2024 to determine that there were no contractors employed by the company	No exceptions noted.



		standard confidentiality agreement.	during the audit window. Inspected the Information Security Policy to determine that the company requires all employees and full-time contractors to sign an industry standard confidentiality agreement. Inspected onboarding documentation to determine that there were no contractors employed by the company during the audit window.	No exceptions noted. Not tested, did not occur during observation.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inquired of the President on May 2, 2024 to determine that no employees were on-boarded during the audit window. Inspected the Information Security Policy to determine that the company requires employees to sign a confidentiality agreement during onboarding. Inspected onboarding documentation to determine that no employees were on-boarded during the audit window.	No exceptions noted. No exceptions noted. Not tested, did not occur during observation.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company's management documents performance evaluations for each employee to provide feedback on performance at least annually.	Inquired of the President/CEO on May 2, 2024 to determine that the company does not have any formal employees and therefore performance evaluations are not required at this time. Inspected the Performance Review Policy to determine that the company's management documents performance evaluations for each employee to provide feedback on performance at least annually. Volunteers may opt-out of the formal review process.	Not tested, did not occur during observation. No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually. The board provides feedback and direction to management as needed.	Inspected the board of directors meeting minutes from a meeting held in December 2023 to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually. The board provides feedback and direction to management as needed.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's bylaws to determine that they document the board's responsibility to manage all the business affairs of the company.	No exceptions noted.



CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	<p>Inspected the resumes of the board members showing their experiences, skills, and qualifications to determine that the board of directors has adequate expertise to lead the management team and oversee the company's internal controls.</p> <p>Inspected the penetration test from Q1 2024 to determine that the company's board engages third-party information security experts and consultants as needed.</p>	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least quarterly and maintains formal meeting minutes.	Inspected the meeting minutes for a sample of quarterly board meetings held during the audit period to determine that the company's board of directors meets at least quarterly and maintains formal meeting minutes.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's bylaws to determine that they document the board's responsibility to manage all the business affairs of the company.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected an organizational chart which includes organization structure and reporting lines to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the job summaries from the Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	<p>Inquired of the President on May 2, 2024 to determine that the company does not have any employees therefore performance reviews are not required.</p> <p>Observed that the company does not have any paid employees who require performance review.</p>	Not tested, did not occur during observation.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain	The company performs background checks on new employees.	Inquired of the President on May 2, 2024 to determine that no employees were on-boarded during the audit window.	Not tested, did not occur during observation.



	competent individuals in alignment with objectives.		Inspected the onboarding documentation to determine that there were no employees onboarded during the audit window.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company has a security awareness training program in-place for all applicable personnel. All applicable personnel complete the training and completion of such training is logged.	Inspected the security awareness training logs to determine that the company has a security awareness training program in-place for all applicable personnel. All applicable personnel complete the training and completion of such training is logged.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the job summaries from the Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inquired of the President on May 2, 2024 to determine that no employees were on-boarded during the audit window. Inspected onboarding documentation to determine that there were no employees onboarded during the audit window.	Not tested, did not occur during observation.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inquired of the President on May 2, 2024 to determine that the company does not have any employees therefore performance reviews are not required. Observed that the company does not have any paid employees who require performance review.	Not tested, did not occur during observation.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the job summaries from the Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the self control assessment review performed in January 2024, to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	No exceptions noted.



			Corrective actions are taken based on relevant findings.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log activity document from the various systems to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the job summaries from the Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized internal users.	Inspected the Github commit page where developers share communication to determine that the company communicates system changes to authorized internal users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspect the company master policy document which includes the information security policy to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and	The company requires employees to complete	Inquired of the President on May 2, 2024 to determine that there were no employees onboarded during the audit	Not tested, did not



	responsibilities for internal control, necessary to support the functioning of internal control.	security awareness training within thirty days of hire.	window. Inspected onboarding documentation to determine that there were no employees onboarded during the audit window.	occur during observation.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Roles and Responsibilities Policy to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has an email available to receive disclosures of incidents or system failures. The email is publicly listed on the company's security page.	Inspected the customer feedback evidence document to determine that the company has provided an email address for the customer on the feedback section of the website to send feedback, disclosures of incidents or system failures.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has a Security Incident Response Plan in place to deal with security incidents.	Inspected the Security Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the network architecture diagram to determine that a description of the service delivery process is shared with internal users. Inspected an export from the company's website on February 13, 2024 to determine that the company provides a description of its products and services through its website.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Terms of Service and Privacy Policies for a sample of vendors and the Microsoft business associate agreement to determine that the vendors' data protection and security commitments are formally acknowledged in an agreement.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected an online contact form on the company's website to determine that the company provides users with an external-facing support system to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting	The company provides guidelines and technical support resources relating to	Inquired of the President on May 2, 2024 to determine that the company provides guidelines and technical support resources relating to system operations	No exceptions noted.



	the functioning of internal control.	system operations to customers.	to customers. Inspected the company's technical support implementation guide to determine that the company provides guidelines and technical support resources relating to system operations to customers. Observed a video demonstration on the company's website to determine that the company provides guidelines and technical support resources relating to system operations to customers.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inquired of the President on May 2, 2024 to determine that there were no critical changes that occurred during the audit window. Inspected the change log tracker from during the audit window to determine that no critical changes occurred during the audit period to necessitate customer notification.	Not tested, did not occur during observation.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected a services agreement template to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the network architecture diagram to determine that a description of the service delivery process is shared with internal users. Inspected an export from the company's website on February 13, 2024 to determine that the company provides a description of its products and services through its website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a risk assessment policy in place to guide it during its risk assessments, which are completed at least annually.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.



CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A formal Risk Assessment is completed at least annually and as needed in accordance with the risk management policy.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the security review reports of the vendors to determine that the company evaluates vendor performance and compliance with contractual obligations.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A formal Risk Assessment is completed at least annually and as needed in accordance with the risk management policy.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.



		associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Independent third-party penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	Inspected the penetration test report from within the audit window to determine that penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the configuration management settings as well as the log of configurations deployed during the observation window to determine that the company ensures that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A formal Risk Assessment is completed at least annually and as needed in accordance with the risk management policy.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Independent third-party penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	Inspected the penetration test report from within the audit window to determine that penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the security review reports of the vendors to determine that the company evaluates vendor performance and compliance with contractual obligations.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations	The company performs control self-assessments at least annually to gain assurance that	Inspected the self control assessment review performed in January 2024, to determine that the company performs	No exceptions noted.



	to ascertain whether the components of internal control are present and functioning.	controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the security review reports of the vendors to determine that the company evaluates vendor performance and compliance with contractual obligations.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the self control assessment review performed in January 2024, to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspect the company master policy document which includes the information security policy to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.



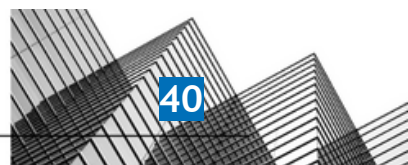
		associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspect the company master policy document which includes the information security policy to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a Change Management Policy governing the system development life cycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy to determine that the company has described secure system engineering principles, and change control procedures.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and Termination Policy in addition to the dashboards of the various systems to determine that the company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the change management process and a sample of change tickets to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company performs backups of customer data at least daily, where available. Backups are retained in accordance with the company Business Continuity and Disaster Recovery Plan.	Inspected the database backup logs from within the audit window to determine that the company performs backups of customer data at least daily, where available. Backups are retained in accordance with the company Business Continuity and Disaster Recovery Plan.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Retention and Disposal Policy to determine that internal data retention and disposal procedures have been established stating that the company is required to retain data as long as the Client is under contract with the Company. If data disposal is required, secure deletion through the cloud provider will be used.	No exceptions noted.



CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspect the company master policy document which includes the information security policy to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a Security Incident Response Plan in place to deal with security incidents.	Inspected the Security Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the job summaries from the Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the security review reports of the vendors to determine that the company evaluates vendor performance and compliance with contractual obligations.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a Change Management Policy governing the system development life cycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy to determine that the company has described secure system engineering principles, and change control procedures.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a risk assessment policy in place to guide it during its risk assessments, which are completed at least annually.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment	No exceptions noted.



			review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	
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.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the Microsoft Entra Id dashboard and production system login history to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the application to authorized users with a business need.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company restricts privileged access to the application to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains an inventory of assets, including system components and company devices.	Inspected the evidence of Azure assets including SQL database, SQL server, virtual network, and other assets to determine that the company maintains an inventory of assets, including system components and company devices.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company restricts privileged access to databases to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms such as Multi-factor authentication.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to production datastores to use authorized secure authentication mechanisms such as Multi-factor authentication.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that company restricts privileged access to the firewall to authorized users with a business need.	No exceptions noted.



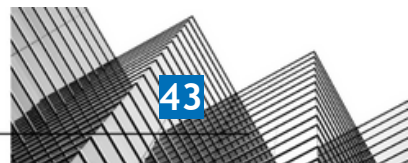
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the Azure configurations for transparent data encryption showing encrypted status to determine that the company's data stores housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has established policies for password strength and authentication requirements. Such policy requires that passwords have at least 8 characters and the use of uppercase, lowercase and a number.	Inspected the Microsoft password complexity requirements to determine that the company's Password policies are set by the 3rd party federated authentication providers.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company restricts privileged access to the production network to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access requests received and approved during the audit period to determine that user access to in-scope system components is effectively managed through documented access request forms with manager approval before provisioning access.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires approval from one or more independent engineers prior to deploying a change into production. Changes cannot be deployed without independent approval.	Inspected the Change Management Process which includes a population of changes from GitHub to determine that the company requires approval from one or more independent engineers prior to deploying a change into production.	No exceptions noted.



	security events to meet the entity's objectives.		Changes cannot be deployed without independent approval.	
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.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Classification Policy to determine that the company has established a data classification scheme and handling procedures for critical, private, and unrestricted data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company restricts privileged access to operating systems to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's up-to-date encryption certificates which are set to auto-renew to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and Termination Policy in addition to the dashboards of the various systems to determine that the company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access requests received and approved during the audit period to determine that user access to in-scope system components is effectively managed through documented access request forms with manager approval before provisioning access.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required	Inspected the quarterly user access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is	No exceptions noted.



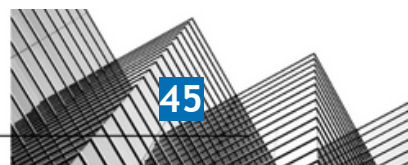
	administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	changes are tracked to completion.	restricted appropriately. Required changes are tracked to completion.	
CC6.2	Prior to issuing system 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.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and Termination Policy in addition to the dashboards of the various systems to determine that the company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Personnel account access for all sensitive systems and applications is revoked within one business day of termination and documented.	Inquired of the President on May 2, 2024 to determine that there were no employee terminations that occurred within the audit window Observed that no client termination had taken place during the audit period.	Not tested, did not occur during observation.
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	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.



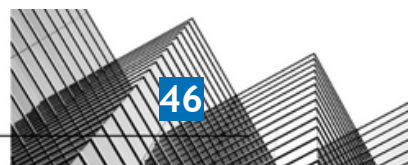
	concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access requests received and approved during the audit period to determine that user access to in-scope system components is effectively managed through documented access request forms with manager approval before provisioning access.	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.	Personnel account access for all sensitive systems and applications is revoked within one business day of termination and documented.	Inquired of the President on May 2, 2024 to determine that there were no employee terminations that occurred within the audit window Observed that no client termination had taken place during the audit period.	Not tested, did not occur during observation.
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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the quarterly user access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	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.	The company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	Inspected the Access Control and Termination Policy in addition to the dashboards of the various systems to determine that the company has an Access Control and Termination Policy that requires unique ID's for access to email, cloud infrastructure, endpoint devices, version control and communication tools.	No exceptions noted.



CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the quarterly user access review report to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Retention and Disposal Policy to determine that internal data retention and disposal procedures have been established stating that the company is required to retain data as long as the Client is under contract with the Company. If data disposal is required, secure deletion through the cloud provider will be used.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Personnel account access for all sensitive systems and applications is revoked within one business day of termination and documented.	Inquired of the President on May 2, 2024 to determine that there were no employee terminations that occurred within the audit window Observed that no client termination had taken place during the audit period.	Not tested, did not occur during observation.
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.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inquired of the President on May 2, 2024 to determine that there were no data deletions within the audit window. Observed that no client termination had taken place during the audit period.	Not tested, did not occur during observation.
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.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inquired of the President on May 2, 2024 to determine that there was no media destruction from within the audit window. Observed that no media destruction had taken place during the audit period.	Not tested, did not occur during observation.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's up-to-date encryption certificates which are set to auto-renew to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.



CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Microsoft Defender for Cloud dashboard and security alerts notification settings to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's up-to-date encryption certificates which are set to auto-renew to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Microsoft Azure Entra Id dashboard and sign in logs to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the annual review of the company's firewalls conducted in January 2024, to determine that the company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the documented standards for Microsoft Azure and Google Workspace hardening documentation to determine that the company assists in maintaining robust security measures and ensures compliance with established standards, as required.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the Microsoft Entra Id dashboard and production system login history to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Inquired of the President on May 2, 2024 regarding removable media to determine that company does not have any removable media. Inspected the encryption settings for a population of devices used by personnel to determine that the company encrypts portable and removable media devices when used.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information	The company uses secure data transmission protocols to encrypt confidential and	Inspected the company's up-to-date encryption certificates which are set to auto-renew to determine that the	No exceptions noted.



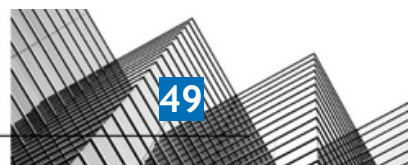
	to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	sensitive data when transmitted over public networks.	company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks.	<p>Inspected the vulnerability and patch management policy to determine that the company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks.</p> <p>Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.</p>	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a Change Management Policy governing the system development life cycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy to determine that the company has described secure system engineering principles, and change control procedures.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	<p>Inquired of the President on May 2, 2024 regarding anti-malware technologies to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.</p> <p>Inspected the anti-malware settings for both the windows environment in addition to the macOS environment to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.</p>	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to	The company's formal policies outline the requirements for the following functions related to IT/Engineering:	Inspected the Vulnerability and Patch Management Policy to determine that the company's formal policies outline the requirements for the following functions	No exceptions noted.



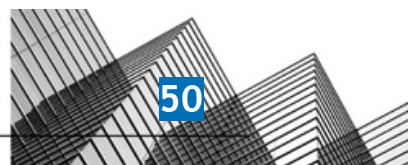
	configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	- vulnerability management; - system monitoring.	related to IT/Engineering: - vulnerability management; - system monitoring.	
CC7.1	To meet its objectives, the entity uses 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.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the configuration management settings as well as the log of configurations deployed during the observation window to determine that the company ensures that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the change management process and a sample of change tickets to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A formal Risk Assessment is completed at least annually and as needed in accordance with the risk management policy.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those	The company's formal policies outline the requirements for the following functions related	Inspected the Vulnerability and Patch Management Policy to determine that the company's formal policies outline the	No exceptions noted.



	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.	to IT/Engineering: - vulnerability management; - system monitoring.	requirements for the following functions related to IT/Engineering: - vulnerability management; - system monitoring.	
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.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Independent third-party penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	Inspected the penetration test report from within the audit window to determine that penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log activity document from the various systems to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.



CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Microsoft Defender for Cloud dashboard and alerts center to determine that an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks.	Inspected the vulnerability and patch management policy to determine that the company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Microsoft Defender for Cloud dashboard and security alerts notification settings to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management parties according to the company's security incident response policy and procedures.	Inquired of the President on May 2, 2024 to determine that there were no security or privacy incidents that were reported during the audit window. Observed that no security incidents were reported during the audit period.	Not tested, did not occur during observation.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the	The company has a Security Incident Response Plan in place to deal with security incidents.	Inspected the Security Incident Response Plan to determine that the company has documented the procedures to assess	No exceptions noted.



	entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		and respond to an information security incident.	
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.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has a Security Incident Response Plan in place to deal with security incidents.	Inspected the Security Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks.	Inspected the vulnerability and patch management policy to determine that the company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the	Inquired of the President on May 2, 2024 to determine that there were no security or privacy incidents that were reported during the audit window. Observed that no security incidents were	Not tested, did not occur during observation.



	communicate security incidents, as appropriate.	company's security incident response policy and procedures.	reported during the audit period.	
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.	The company tests their incident response plan at least annually.	Inspected an Incident Response test report dated January 28, 2024, to determine that the company tests the Incident Response Plan at least annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company has a Business Continuity and Disaster Recovery Plan in place to handle backups, and the steps necessary to recover from potential disasters.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inquired of the President on May 2, 2024 to determine that there were no security or privacy incidents that were reported during the audit window. Observed that no security incidents were reported during the audit period.	Not tested, did not occur during observation.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected an Incident Response test report dated January 28, 2024, to determine that the company tests the Incident Response Plan at least annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a Security Incident Response Plan in place to deal with security incidents.	Inspected the Security Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
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.	The company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks.	Inspected the vulnerability and patch management policy to determine that the company patches its systems in accordance with its Vulnerability and Patch Management Policy to protect from new risks. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	No exceptions noted.



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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the change management process and a sample of change tickets to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the documented standards for Microsoft Azure and Google Workspace hardening documentation to determine that the company assists in maintaining robust security measures and ensures compliance with established standards, as required.	No exceptions noted.
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.	The company requires approval from one or more independent engineers prior to deploying a change into production. Changes cannot be deployed without independent approval.	Inspected the Change Management Process which includes a population of changes from GitHub to determine that the company requires approval from one or more independent engineers prior to deploying a change into production. Changes cannot be deployed without independent approval.	No exceptions noted.
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.	Independent third-party penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	Inspected the penetration test report from within the audit window to determine that penetration tests are performed on production networks and applications annually. Results are assessed and high/critical findings are tracked through remediation.	No exceptions noted.
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.	The company has a Change Management Policy governing the system development life cycle (infrastructure, data, software, and procedures), including procedures for tracking, testing, approving, and validating changes.	Inspected the Change Management Policy to determine that the company has described secure system engineering principles, and change control procedures.	No exceptions noted.
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.	The company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	Inspected the Vulnerability and Patch Management documents to determine that the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation. Inspected the sole high-security issue identified during a scan that occurred during the audit window which was resolved immediately to determine that	No exceptions noted.



			the company performs vulnerability scans on its systems and applications to identify potential vulnerabilities. Results are assessed and the company tracks high/critical findings through remediation.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company implemented a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, including fraud and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine that the risk assessment processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks. Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A formal Risk Assessment is completed at least annually and as needed in accordance with the risk management policy.	Inspected the completed risk assessment review which was performed during the observation window to determine that risk assessments are performed as part of the risk assessment program.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Terms of Service and Privacy Policies for a sample of vendors and the Microsoft business associate agreement to determine that the vendors' data protection and security commitments are formally acknowledged in an agreement.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place for evaluating vendor performance and compliance with contractual obligations.	Inspected the security review reports of the vendors to determine that the company evaluates vendor performance and compliance with contractual obligations.	No exceptions noted.

