



CLARITY BENEFIT SOLUTIONS

REPORT OF CLARITY BENEFIT SOLUTIONS' EMPLOYEE BENEFIT
ADMINISTRATION SYSTEM AND THE SUITABILITY OF THE DESIGN AND
OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY
THROUGHOUT THE PERIOD FROM AUGUST 1, 2024 TO JULY 31, 2025



Clarity Benefit Solutions – SOC 2 Type 2 Table of Contents

Acronym Table	2
Section 1: Independent Service Auditor's Report	3
Section 2: Assertion of the Management of Clarity Benefit Solutions	8
Section 3: Clarity Benefit Solutions' Description of its Employee Benefit Administration System	
Throughout the Period from August 1, 2024 to July 31, 2025	10
Purpose and Scope of Report	11
System Description	11
Company Overview and Services Provided	11
Principal Service Commitments and System Requirements	11
Infrastructure	12
Software	12
People	13
Procedures	13
Data	14
System Boundaries	14
Subservice Organizations	14
Control Environment	18
Integrity and Ethical Values	19
Commitment to Competence	19
Management's Philosophy and Operating Style	19
Organizational Structure	19
Assignment of Authority and Responsibility	20
HR Policies and Practices	20
Risk Assessment	20
In-Scope Trust Service Category	21
Security	21
Trust Service Categories and Related Control Activities	21
Integration with Risk Assessment	21
Selection and Development of Control Activities	21
Significant Changes Throughout the Examination Period	21
Significant Incidents Throughout the Examination Period	22
Information and Communication	22
Information Systems	22
Communication	22
Monitoring	22
User Entity Controls	23
Section 4: Trust Services Categories, Criteria, Related Controls, and Tests of Controls	24
Testing Approach	25
Sampling Approach	25
Trust Services Security Category, Criteria, Related Controls, and Tests of Controls	26

Acronym Table

◇ ACA	Affordable Care Act
◇ AICPA	American Institute of Certified Public Accountants
◇ API	Application Programming Interface
◇ AT	Attestation Standard
◇ CBS	Clarity Benefit Solutions
◇ CEO	Chief Executive Officer
◇ COBRA	Consolidated Omnibus Budget Reconciliation Act
◇ COSO	Committee of Sponsoring Organizations
◇ CPA	Certified Public Accountant
◇ CRM	Customer Relationship Management
◇ CSA	Control Self-Assessment
◇ CSP	Cloud Service Provider
◇ DC	Description Criteria
◇ DR/BC	Disaster Recover/Business Continuity
◇ FSA	Flexible Spending Account
◇ HD	Hard Drive
◇ HR	Human Resources
◇ HRA	Health Reimbursement Arrangement
◇ HRIS	Human Resources Information System
◇ HAS	Health Savings Account
◇ IaaS	Infrastructure-as-a-Service
◇ IT	Information Technology
◇ LLC	Limited Liability Company
◇ MacOS	Macintosh Operating System
◇ MDM	Mobile Device Management
◇ MSP	Managed Service Provider
◇ O365	Microsoft Office 365
◇ OS	Operating System
◇ SaaS	Software-as-a-Service
◇ SDLC	Software Development Lifecycle
◇ SLA	Service Level Agreement
◇ SOC	System and Organization Controls
◇ SSL	Secure Sockets Layer
◇ TLS	Transport Layer Security
◇ TOU	Terms of Use
◇ TSC	Trust Service Category
◇ TSP	Trust Service Principle
◇ VP	Vice President

Section 1: Independent Service Auditor's Report

Independent Service Auditor's Report on the Description of Clarity Benefit Solutions' Employee Benefits Administration System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

To: Management of Clarity Benefit Solutions,

Scope

We have examined Clarity Benefit Solutions' (the "Company," "Organization," "CBS," or "Clarity") accompanying description of its Employee Benefits Administration system (the "System") found in Section 3 titled, "Clarity Benefit Solutions' Description of its Employee Benefits Administration System Throughout the Period from August 1, 2024 to July 31, 2025" (description)) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period from August 1, 2024 to July 31, 2025, to provide reasonable assurance that Clarity Benefit Solutions' service commitments and system requirements were achieved based on the Trust Services Criteria relevant to security (applicable Trust Services Criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

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

Clarity Benefit Solutions uses subservice organizations for benefit administration, IaaS, benefit enrollment and ACA, benefit management, MSP and CSP, continuous security and compliance monitoring, and COBRA benefit management services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Clarity Benefit Solutions, to achieve Clarity Benefit Solutions' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Clarity Benefit Solutions' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Clarity Benefit Solutions' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

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

Inherent Limitations

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

Description of Tests of Controls

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

Clarity Benefit Solutions' description of its system discusses the following controls which were in place and appropriately designed during the examination period from August 1, 2024 to July 31, 2025. However, these controls were not tested for operating effectiveness, as no relevant events or circumstances occurred that required their operation during the examination period.

- ◇ The Company's security 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.

Opinion

In our opinion, in all material respects:

- a. The description presents Clarity Benefit Solutions' Employee Benefits Administration system that was designed and implemented throughout the period from August 1, 2024 to July 31, 2025 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period from August 1, 2024 to July 31, 2025 to provide reasonable assurance that Clarity Benefit Solutions' service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Clarity Benefit Solutions' controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period from August 1, 2024 to July 31, 2025 to provide reasonable assurance that Clarity Benefit Solutions' service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organizations controls assumed in the design of Clarity Benefit Solutions' controls operated effectively throughout that period.

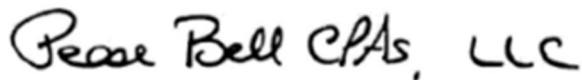
Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Clarity Benefit Solutions, user entities of Clarity Benefit Solutions' Employee Benefits Administration system during some or all of the period from August 1, 2024 to July 31, 2025, business partners of Clarity Benefit Solutions subject to risks arising from interactions with the Employee Benefits Administration system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Pease Bell CPAs, LLC



September 8, 2025

Akron, Ohio

Section 2: Assertion of the Management of Clarity Benefit Solutions

Assertion of the Management of Clarity Benefit Solutions

We have prepared the accompanying description of Clarity Benefit Solutions' (the "Company," "Organization," "CBS," or "Clarity") Employee Benefits Administration system (the "System") titled, "Clarity Benefit Solutions Employee Benefits Administration System Throughout the Period from August 1, 2024 to July 31, 2025" (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Employee Benefits Administration system that may be useful when assessing the risks arising from interactions with Clarity Benefit Solutions' system, particularly information about system controls that Clarity Benefit Solutions 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 (applicable Trust Services Criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Clarity Benefit Solutions uses subservice organizations to provide benefit administration, laaS, benefit enrollment and ACA, benefit management, MSP and CSP, continuous security and compliance monitoring, and COBRA benefit management services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Clarity Benefit Solutions, to achieve Clarity Benefit Solutions' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Clarity Benefit Solutions' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Clarity Benefit Solutions' controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Clarity Benefit Solutions, to achieve Clarity Benefit Solutions' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the service organization's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

- 1) The description presents Clarity Benefit Solutions' Employee Benefits Administration system that was designed and implemented throughout the period from August 1, 2024 to July 31, 2025 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period from August 1, 2024 to July 31, 2025 to provide reasonable assurance that Clarity Benefit Solutions' service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Clarity Benefit Solutions' controls throughout that period.
- 3) The controls stated in the description operated effectively throughout the period from August 1, 2024 to July 31, 2025 to provide reasonable assurance that Clarity Benefit Solutions' service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organizations controls and complementary user entity controls assumed in the design of Clarity Benefit Solutions' controls operated effectively throughout that period.
- 4) The Company's description of its system discusses the following controls that did not operate within the period from July 1, 2024 to June 30, 2025 due to no occurrence of the activity to test the operating effectiveness:
 - ◇ The Company's security 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.

/s/ Shailaja Srivastava
VP of Information Technology
Clarity Benefit Solutions
September 8, 2025

**Section 3: Clarity Benefit Solutions' Description of its Employee
Benefit Administration System Throughout the Period from
August 1, 2024 to July 31, 2025**

Purpose and Scope of Report

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of Clarity Benefit Solutions' controls that may be relevant to a user entity's internal control structure. This report, when combined with an understanding of the policies and procedures at user entities, is intended to assist user auditors in planning the audit of the user entities and in assessing control risk for assertions of the user entities that may be affected by policies and procedures of Clarity Benefit Solutions' Employee Benefits Administration system.

This report describes the system and control structure of Clarity Benefit Solutions as they relate to the Employee Benefits Administration system. It is intended to assist user entities and their independent auditors in determining the adequacy of the internal controls that are outsourced to Clarity Benefit Solutions and are relevant to their internal control structures as it relates to security risks. This document was prepared in accordance with the guidance contained in the AICPA AT Section 101 – Attest Engagements.

Clarity Benefit Solutions uses subservice organizations for benefit administration, IaaS, benefit enrollment and ACA, benefit management, MSP and CSP, continuous security and compliance monitoring, and COBRA benefit management services.

This description is intended to focus on the internal control structure of Clarity Benefit Solutions that is relevant to only users of Clarity Benefit Solutions' Employee Benefits Administration system and does not encompass all aspects of the services provided or procedures followed by Clarity Benefit Solutions.

System Description

Company Overview and Services Provided

Clarity Benefit Solutions, founded in 1990, is a financial services provider headquartered in Clark, New Jersey that provides benefits administration services to employers across many industries. Clarity Benefit Solutions' goal has been to use technology to simplify the administration of benefits, reduce costs, and empower consumers. In the beginning, the Company was known as BeneFlex, one of the first providers of Flexible Benefit Plans. Over the years, Clarity Benefit Solutions has expanded their services to include various pretax consumer benefits, online enrollment, HRIS, and mobile technology. Clarity brings benefits to focus by combining all their offerings into one platform. Clarity offers cloud-based software and backs it with skilled customer service.

Principal Service Commitments and System Requirements

Clarity Benefit Solutions designs its processes and procedures related to the Employee Benefits Administration system to meet its objectives. Those objectives are based on the service commitments that Clarity Benefit Solutions makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Clarity Benefit Solutions has established for the services.

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

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

Clarity Benefit Solutions establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Clarity Benefit Solutions' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Employee Benefits Administration system.

Infrastructure

Clarity Benefit Solutions is a third-party administrator of health benefits and utilizes third-party systems to connect and manage their client's benefit needs.

- ◇ Alegeus provides a Consumer-Directed Health plan administration platform called the WealthCare Administration System.
- ◇ Bswift was a subsidiary of Aetna Health holdings and provided benefits enrollment and administration for employers.
- ◇ Employee Navigator was a SaaS provider that Clarity used to manage benefits, onboarding, and ACA.
- ◇ Alegeus WealthCare COBRA system are used for COBRA and direct bill for clients through their online elections and open enrollment application.

Clarity relies on the infrastructure of the third-party systems listed above to provide secure, available, and integration services to support the needs of their clients.

Clarity uses Two River Technology Group to host the corporate infrastructure that is needed to provide the Employee Benefits Administration system. Two River Technology Group is the MSP and cloud provider used to manage the corporate environment hosted in Microsoft Azure. O365 accounts are provisioned for each Clarity employee, and access to certain files and resources is restricted to users based on job functions. Employee workstations are a combination of Windows and MacOS operating systems with hard drive encryption and antivirus enabled for workstations. Two River Technology Group is responsible for the security, availability, and integrity of the corporate environment and cloud resources they host for Clarity.

Software

The following provides a summary of systems used to deliver the Employee Benefits Administration system:

- ◇ Alegeus provides a Consumer-Directed Health plan administration platform called the WealthCare Administration System.
- ◇ Bswift was a subsidiary of Aetna Health holdings and provided benefits enrollment and administration for employers.
- ◇ Employee Navigator was a SaaS provider that Clarity used to manage benefits, onboarding, and ACA.
- ◇ Alegeus WealthCare COBRA system is used for COBRA and direct bill for clients through their online elections and open enrollment application.
- ◇ Microsoft Office products are used as corporate productivity tools such as Word, Excel, Outlook, and Teams.
- ◇ Microsoft Teams is used as an internal communication tool.
- ◇ O365 is used as the identity provider to manage authentication and access controls to production systems and applications.

- ◇ Vanta is used as a continuous security and compliance monitoring device.
- ◇ CrowdStrike is used for antivirus protection on workstations and cloud instances.
- ◇ Microsoft Defender is used for antivirus coverage on Azure-hosted instances.

People

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

- ◇ CEO, who is responsible for leading and overseeing overall Company operations, including finance, HR, sales, marketing, operations and service delivery.
- ◇ Chief Marketing Officer, who is responsible for helping grow Clarity's market share, drive thought leadership, enhance Clarity's online reputation and brand equity and grow the Company's overall revenue.
- ◇ Senior VP of Sales, who is responsible for shaping and growing Clarity's sales initiatives to achieve the vision of the Company, create and strengthen key partnerships, and grow overall Company revenue.
- ◇ VP of Consumer Benefit Implementation & Renewal, who is responsible for providing leadership, strategic direction and guidance to the Implementation and Renewal Teams with a focus on successful client experiences and superior client service.
- ◇ VP of HR, who is responsible for employee onboarding/offboarding, employee relations, performance management, personnel policy analysis and implementation. The VP of HR is also responsible for oversight of recruitment, talent acquisitions, and employee engagement.
- ◇ VP of Information Technology, who is responsible for oversight of IT related hardware, software, configuration, and security. The VP IT is also responsible for the strategic growth and implementation of Clarity's technology and digital presence in the benefits market.
- ◇ VP of Service, who is responsible for providing leadership, strategic direction and guidance to the Employer and Participant Services Teams with a focus on effortless service and speed to answer.

Procedures

Executive and Operations Management personnel maintain documented operating procedures involved in the operation of Clarity Benefit Solutions' Employee Benefit Administration system that include:

- ◇ Asset Management Policy
- ◇ Code of Conduct
- ◇ Confidential Data Policy
- ◇ Cryptography Policy
- ◇ Disaster Recovery/Business Continuity Plan
- ◇ Incident Response Policy
- ◇ Information Security Policy
- ◇ Information Security Roles and Responsibilities Policy
- ◇ Network Access and Authentication Policy
- ◇ Operations Security Policy
- ◇ Outsourcing Policy
- ◇ Physical Security Policy
- ◇ Risk Management Policy
- ◇ Secure Development Policy

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which Clarity Benefit Solutions strives to achieve its business objectives. Clarity

Benefit Solutions has applied a risk management approach to the Organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved, when necessary, to meet the applicable Trust Services Criteria and the overall objective of the Organization.

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

Data

Clarity Benefit Solutions' Employee Benefits Administration system comes in contact with many forms of data. Clarity's Data Management Policy defines five data classification categories: personal, public, operational, critical, and confidential. Data storage policies are defined based on the category of the data.

Clarity Benefit Solutions data in storage is encrypted at rest. In addition, Clarity Benefit Solutions protects the transmission of confidential data using a combination of SSL certificates and TLS. Electronic data is protected via logical access controls and network protection devices, with the production systems segregated from the corporate network.

System Boundaries

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

Subservice Organizations

Clarity Benefit Solutions relies on subservice organizations to create efficiencies in the Employee Benefits Administration System. Clarity Benefit Solutions monitors the service commitments made by the subservice organizations in an annual vendor management program. Clarity Benefit Solutions obtains attestation reports, or other relevant information, and reviews the controls and test results to help ensure the subservice organization's service commitments are met. Remediation plans and monitoring timelines are implemented if testing exceptions were discovered in Clarity Benefit Solutions' review of the attestation reports. The table below summarizes the subservice organizations in use by Clarity Benefit Solutions and the services provided.

Subservice Organization	Services Provided to Clarity Benefit Solutions
Alegeus	SaaS (WealthCare Administration System)
Bswift	Benefit enrollment and administration services
Employee Navigator	SaaS (benefit management, onboarding and ACA)
Microsoft Azure	IaaS (Corporate)
Two River Technology Group	MSP and CSP
Vanta	Continuous security and compliance monitoring
WealthCare COBRA	COBRA benefit management

Alegeus

Clarity Benefit Solutions uses Alegeus' benefit administration application, WealthCare Administration System, to support its client's needs related to FSAs, HSAs, HRAs, wellness incentives, dependent care, and commuter accounts. Alegeus is responsible for the logical security of the web application used by Clarity Benefit Solutions' clients. Alegeus is also responsible for the security, availability, and integrity of the data transmitted or stored within the WealthCare Administration System.

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

Control Activity Expected to be Implemented by Alegeus	Applicable Trust Services Criteria
Alegeus is responsible for the security, confidentiality, and integrity of the information and data created, stored or transferred via the WealthCare Administration web application.	CC4.1, CC5.2, CC6.7
Alegeus is responsible for the security of the WealthCare Administration web application specific to Clarity Benefit Solutions and limiting access to only those with business justification to the web application.	CC6.1, CC6.2
Alegeus is responsible for encrypting client credentials at rest and restricting decryption access.	CC6.6, CC6.7
Alegeus is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Azure

Clarity Benefit Solutions uses Azure to host their corporate systems used to provide the Employee Benefits Administration system. The Azure resources and services are hosted and maintained by Two River Technology Group. Azure provides IaaS network security, database, storage, and application services for Clarity Benefit Solutions.

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

Control Activity Expected to be Implemented by Azure	Applicable Trust Services Criteria
Azure is responsible for restricting logical and physical access to and within the data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.8
Azure is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Azure is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4
Azure is responsible for the management of any third-party vendors with access to customer environments.	CC9.2

Bswift

Bswift was a subsidiary of Aetna Health holdings and provided benefits enrollment and administration for employers. Clarity Benefit Solutions used Bswift's HR Benefits Administration system for consumer benefit information. Bswift was responsible for the logical security of the web application used by Clarity Benefit Solutions' clients. Bswift was also responsible for the security, availability, and integrity of the data transmitted or stored within the HR Benefits Administration system.

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

Control Activity Expected to be Implemented by Bswift	Applicable Trust Services Criteria
Bswift is responsible for the security, confidentiality, and integrity of the information and data created, stored or transferred via the HR Benefits Administration system.	CC4.1, CC5.2, CC6.7
Bswift is responsible for the security of the HR Benefits Administration system specific to Clarity Benefit Solutions and limiting access to only those with business justification to the web application.	CC6.1, CC6.2
Bswift is responsible for encrypting client credentials at rest and restricting decryption access.	CC6.6, CC6.7
Bswift is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Employee Navigator

Clarity Benefit Solutions used Employee Navigator's hosted Benefits Enrollment Services system to provide the licensed software to Clarity Benefit Solutions' team members and their client companies. Employee Navigator was responsible for the logical security of the web application used by Clarity Benefit Solutions' team members and client companies. Employee Navigator was also responsible for the security, availability, and integrity of the data transmitted or stored within the Employee Navigator software.

The applicable Trust Services Criteria that are intended to be met by controls at Employee Navigator, alone or in combination with controls at Clarity Benefit Solutions, and the types of controls expected to be implemented at the subservice organization to meet those Trust Service Criteria are described in the section below:

Control Activity Expected to be Implemented by Employee Navigator	Applicable Trust Services Criteria
Employee Navigator is responsible for the security, confidentiality, and integrity of the information and data created, stored or transferred via the Employee Navigator software.	CC4.1, CC5.2, CC6.7
Employee Navigator is responsible for the security of the Employee Navigator software specific to Clarity Benefit Solutions and limiting access to only those with business justification to the web application.	CC6.1, CC6.2
Employee Navigator is responsible for encrypting client credentials at rest and restricting decryption access.	CC6.6, CC6.7

Control Activity Expected to be Implemented by Employee Navigator	Applicable Trust Services Criteria
Employee Navigator is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Two River Technology Group

Clarity Benefit Solutions uses Two River Technology Group as their CSP to provide managed cloud services for the Azure environment. Two River Technology Group's team of certified engineers build, manage, and automate enterprise workloads within Clarity Benefit Solutions Azure infrastructures. Two River Technology Group is responsible for ongoing change management and event response to help ensure the Azure environments are protected over time.

The applicable Trust Services Criteria that are intended to be met by controls at Two River Technology Group, alone or in combination with controls at Clarity Benefit Solutions, and the types of controls expected to be implemented at the subservice organization to meet those Trust Service Criteria are described in the section below:

Control Activity Expected to be Implemented by Two River Technology Group	Applicable Trust Services Criteria
Two River Technology Group is responsible for restricting logical access to and within the data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.6, CC6.8
Two River Technology Group is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2, CC7.1
Two River Technology Group is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4
Two River Technology Group is responsible for the management of any third-party vendors with access to customer environments.	CC9.2

Vanta

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

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

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

WealthCare COBRA

Clarity Benefit Solutions uses WealthCare COBRA's health account services and platform to support its client companies' needs related to COBRA enrollment. WealthCare COBRA is responsible for the logical security of the platform used by Clarity Benefit Solutions' clients. WealthCare COBRA is also responsible for the security, availability, and integrity of the data transmitted or stored within its platform.

The applicable Trust Services Criteria that are intended to be met by controls at WealthCare COBRA, alone or in combination with controls at Clarity Benefit Solutions, and the types of controls expected to be implemented at the subservice organization to meet those Trust Service Criteria, are described in the section below:

Control Activity Expected to be Implemented by WealthCare COBRA	Applicable Trust Services Criteria
WealthCare COBRA is responsible for the security, confidentiality, and integrity of the information and data created, stored or transferred via the Health Cloud platform.	CC4.1, CC5.2, CC6.7
WealthCare COBRA is responsible for the security of the Health Cloud platform specific to Clarity Benefit Solutions and limiting access to only those users with business justification to access the web application.	CC6.1, CC6.2
WealthCare COBRA is responsible for encrypting client credentials at rest and restricting decryption access.	CC6.6, CC6.7
WealthCare COBRA is responsible for notifying Clarity Benefit Solutions of any suspected or actual security incidents and containing, remediating, and communicating security incidents as appropriate.	CC7.3, CC7.4

Control Environment

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

The control environment at Clarity Benefit Solutions begins with Management's philosophy and operating style as well as the priorities and direction provided by the Executive Management Team. Clarity Benefit Solutions' entire organization is dedicated to delivering the highest level of customer service. The Company has created a corporate culture that supports this mission. The Company's Executive Management Team meets at least annually to discuss the state of the Company's cybersecurity and privacy risk.

Integrity and Ethical Values

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

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

Commitment to Competence

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

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

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics include the following: Management's approach to taking and monitoring business risk, and Management's attitude and actions for the security and confidentiality of information. Clarity Benefit Solutions' Management takes a conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

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

The responsibilities of key positions within Clarity Benefit Solutions are clearly defined and communicated to personnel. Individuals that hold key positions are knowledgeable and experienced within the industry. Clarity Benefit Solutions' organizational structure supports the communication of information both up to leadership as well as down to support staff. Clarity Benefit Solutions' organizational structure is comprised of six primary business units that work together to deliver the Employee Benefits Administration system.

The six business units consist of:

- ◇ Executive Management – Responsible for defining business objectives, information security, and operational procedures.
- ◇ Client Services – Responsible for customer support and current client success.
- ◇ Technology – Responsible for oversight of IT related hardware, software, configuration, security, and oversight of functions as they relate to the implementation and servicing of Clarity's clients.
- ◇ Accounting/ Finance – Responsible for record keeping for accounting purposes and for current and projected financial models.
- ◇ HR – Responsible for recruitment, talent acquisitions, and employee engagement.
- ◇ Sales and Marketing – Responsible for shaping and growing Clarity's sales initiatives to achieve the vision of the Company, create and strengthen key partnerships, and grow overall Company revenue.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions, and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge, and experience required of key personnel and the appropriate number of people to carry out duties. In addition, Management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

HR Policies and Practices

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

Risk Assessment

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in its description of the Employee Benefits Administration system. Clarity Benefit Solutions' Management has implemented a process for identifying relevant risks to take place annually.

The risk assessment process consists of the following phases:

- ◇ Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- ◇ Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- ◇ Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- ◇ Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.

- ◇ Monitoring – The monitoring phase includes the performance of monitoring activities by Clarity Benefit Solutions’ Management team to evaluate whether the processes, initiatives, functions and/or activities are mitigating the risk as designed.

In-Scope Trust Service Category

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

Trust Services Category	Definition
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity’s ability to achieve its objectives.

Security

Security refers to the protection of:

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

Trust Service Categories and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, Clarity Benefit Solutions’ Management has identified and put into effect the necessary actions to address those risks. In order to address these risks, control activities have been placed into operation to help ensure that the actions are carried out in a competent and efficient manner. Control activities serve as various mechanisms for managing the achievement of the security principle and applicable criteria.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in the control matrices within Section 4 of this report to eliminate the redundancy that would result from listing the items in this section. Although the control activities are included in the testing matrices set forth below in Section 4, they are, nevertheless, an integral part of Clarity Benefit Solutions’ description of its Employee Benefits Administration system. Any applicable Trust Services Criteria that are not addressed by control activities at Clarity Benefit Solutions are also described within the control matrices.

Significant Changes Throughout the Examination Period

In October 2024, Clarity Benefit Solutions sold its benefits administration business to PES Benefits. This change marked a transition away from Clarity’s prior use of third-party vendors Bswift and Employee Navigator, which had previously supported benefits enrollment, administration, onboarding, and ACA compliance functions. Following the sale, Clarity no longer maintains access to these platforms or the associated data. This transition represents a material change in the system boundaries and subservice

organization relationships relevant to the scope of this examination. Controls previously operated by Bswift and Employee Navigator are no longer in effect for Clarity Benefit Solutions as of the sale date.

Significant Incidents Throughout the Examination Period

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

Information and Communication

Information Systems

Clarity Benefit Solutions' Employee Benefits Administration system is a SaaS platform used by Clarity Benefit Solution's employees and their client companies to manage employee benefits. The Employee Benefits Administration system combines access to many third-party systems and resources so the client companies can efficiently and effectively manage their employees' benefit packages. Clarity Benefit Solutions does not store or maintain any client information within a database or other storage solutions. Client company information is stored, transmitted, or retained by third-party software solutions. (See subservice organizations above).

Communication

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

Monitoring

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

Management strives to be proactive in responding to customer complaints and maintains a high level of inter-departmental communication about these events. Customer complaints and other issues are handled via personal contact by Clarity Benefit Solutions' Customer Support Team, and are forwarded to the legal department, if necessary.

User Entity Controls

The control activities performed by Clarity Benefit Solutions cover only a portion of the overall internal control structure of Clarity Benefit Solutions' user entities. Therefore, each customer's internal control structure must be evaluated in conjunction with Clarity Benefit Solutions' control policies and procedures described in this report. Clarity Benefit Solutions' controls over its Employee Benefit Administration system were designed with the understanding that certain user entity controls were in place and operating effectively.

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for maintaining their access to, and segregating duties within, the Employee Benefit Administration system.	CC6.1
User entities are responsible for evaluating the physical security and logical security of devices that access the Clarity Benefit Solutions' services and reside at their operational facilities. User entities should consider the controls over sharing, downloading, editing, creating, and deleting of their data.	CC6.7
User entities are responsible for immediately notifying Clarity Benefit Solutions of any actual or suspected information security breaches, including compromised user accounts.	CC7.3
User entities are responsible for determining whether Clarity Benefit Solutions' security infrastructure is appropriate for their needs and for notifying the service organization of any requests for modifications.	CC8.1

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

Testing Approach

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

Types of Tests Performed:

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

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by Clarity Benefit Solutions:

Nature of Control and Frequency of Performance	Minimum Number of Items to Test
Occurrence based	10%, minimum of 5, maximum of 25
Manual control performed weekly	5
Manual control performed monthly	2
Manual control performed quarterly	2
Manual control performed annually	1
Application / Programmed control	Test one application of each programmed control for each type of transaction if supported by effective IT general controls (that have been tested); otherwise test at least 25

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

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC1.0	CONTROL ENVIRONMENT				
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	The Company conducts background checks on new employees.	Inspected the completed background check for a sample of new hires to verify that the Company performed background checks on new employees.	No exceptions noted.
		CC1.1.2	The Company requires contractor agreements to include a Code of Conduct or reference to the Company Code of Conduct.	Inspected the signed agreement for a sample of new contractors to verify that the Company required contractor agreements to include a reference to the Company Code of Conduct.	No exceptions noted.
		CC1.1.3	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.	Inspected the Code of Conduct and acknowledged Code of Conduct for a sample of new hires to verify that the Company required employees to acknowledge a Code of Conduct at the time of hire and subjected those who violated it to disciplinary actions in accordance with a Disciplinary Policy.	No exceptions noted.
				Inquired of the VP of HR to verify that there were no code of conduct violations.	
		CC1.1.4	The Company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the signed agreement for a sample of new contractors to verify that the Company required contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
		CC1.1.5	The Company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed agreement for a sample of new hires to verify that the Company required employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
		CC1.1.6	The Company Managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to verify that the Company Managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC1.2	COSO Principle 2: The Board of Directors demonstrates independence from Management and exercises oversight of the development and performance of internal control.	CC1.2.1	The Company's Executive Leadership, is briefed by the VP of IT at least annually on the state of the Company's cybersecurity and privacy risk. The Executive Leadership Team has oversight of the execution of the information security risk management program and risk treatments.	Inspected the Clarity Leadership Summit Agenda to verify that the Company's Executive Leadership was briefed by the VP of IT at least annually on the state of the Company's cybersecurity and privacy risk, and that the Executive Leadership Team had oversight of the execution of the information security risk management program and risk treatments.	No exceptions noted.
		CC1.2.2	The Company's Information Security Roles and Responsibilities Policy outlines the oversight responsibilities for internal control.	Inspected the Information Security Roles and Responsibilities Policy to verify that the Company's policy outlined the oversight responsibilities for internal controls.	No exceptions noted.
		CC1.2.3	The Company's Executive Leadership Team members have sufficient expertise to oversee Management's ability to design, implement, and operate information security controls. The Executive Leadership Team engages third-party information security experts and consultants as needed.	Inspected the professional profiles of the Company's Executive Leadership Team to verify that the Company's Executive Leadership Team members had sufficient expertise to oversee Management's ability to design, implement, and operate information security controls. Inquired of the VP of IT to verify that the consulting of a third-party information security expert was completed on an as needed basis.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	The Company Management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to verify that the Company's Management had established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
		CC1.3.2	The Company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart to verify that the Company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.3.3	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 Information Security Roles and Responsibilities Policy and job description for a sample of active roles within the Organization to verify that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities Policy.	No exceptions noted.
		CC1.2.2	See CC1.2.2.		
		CC1.4.1	The Company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the completed security awareness training status for a sample of new hires and active employees to verify that the Company required employees to complete security awareness training within thirty days of hire and at least annually thereafter.	No exceptions noted.
		CC1.1.1 CC1.1.6 CC1.3.3	See CC1.1.1, CC1.1.6, and CC1.3.3.		
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.1.3 CC1.1.6 CC1.3.3	See CC1.1.3, CC1.1.6, and CC1.3.3.		
CC2.0 COMMUNICATION AND INFORMATION					
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.1	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 control set within the continuously monitored trust management platform to verify that the Company performed CSAs on a continuous basis to gain assurance that controls were in place and operating effectively. Inquired of the VP of IT to verify that there were no corrective actions needed based on the CSA.	No exceptions noted.
		CC2.1.2	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 Azure activity log to verify that the Company utilized a log management tool to identify events that might have had a potential impact on the Company's ability to achieve its security objectives.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.1.3	The Company has a Confidential Data Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Confidential Data Policy to verify that a policy was in place to help ensure confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
		CC2.2.1	The Company has an Incident Response Plan that is documented and communicated to authorized users.	Inspected the Incident Response Plan and acknowledgement of the Incident Response Plan for a sample of new hires to verify that a plan was documented and communicated to authorized users.	No exceptions noted.
		CC2.2.2	The Company provides a description of its products and services to internal and external users.	Inspected the Solutions page on the Company website to verify that a description of the Company's products and services were communicated to internal and external users.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal controls.	CC2.2.3	The Company communicates system changes to authorized internal users.	Inspected the internal communication system to verify that the Company communicated system changes to authorized internal users.	No exceptions noted.
		CC2.3.1	The Company's security commitments are communicated to customers in TOU.	Inspected the TOU on the Company website to verify that the Company's security commitments were communicated to customers in TOU.	No exceptions noted.
		CC2.3.2	The Company provides guidelines and technical support resources relating to system operations to customers.	Inspected the support page on the Company website to verify that the Company provided guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
		CC2.3.3	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 the support page on the Company website to verify that the Company had an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
		CC2.3.4	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 Outsourcing Policy and the signed agreement for a sample of critical vendors to verify that the Company had written agreements with vendors and related third parties, which included confidentiality and privacy commitments applicable to those entities.	No exceptions noted.
CC3.0	RISK ASSESSMENT				
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.1	The Company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy and completed risk assessment to verify that the Company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
		CC3.1.2	The Company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy and completed risk assessment to verify that the Company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.1	The Company has a documented DR/BC Plan and tests it at least annually.	Inspected the Disaster Recovery/Business Continuity Plan and the DR/BC test results to verify that there was a documented plan and it was tested annually.	No exceptions noted.
		CC3.2.2	The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the completed risk assessment to verify that the Company's risk assessments were performed at least annually, identifying threats and changes to service commitments, formally assessing risks, and considering the potential for fraud and its impact on achieving objectives.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.2.3	<p>The Company has a vendor management program in place. Components of this program include:</p> <ul style="list-style-type: none"> ◇ Critical third-party vendor inventory; ◇ Vendor's security and privacy requirements; and ◇ Review of critical third-party vendors at least annually. 	Inspected the Outsourcing Policy, vendor inventory, completed vendor assessments, and attestation reports for a sample of vendors categorized as critical to verify that the Company had a vendor management program in place, which included a critical third-party vendor inventory, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
		CC3.1.1 CC3.1.2	See CC3.1.1 and CC3.1.2.		
		CC3.1.1 CC3.1.2 CC3.2.2	See CC3.1.1, CC3.1.2, and CC3.2.2.		
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.1.2 CC3.2.2	See CC3.1.2 and CC3.2.2.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC4.0	MONITORING ACTIVITIES				
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC2.1.1 CC3.2.2 CC3.2.3	See CC2.1.1, CC3.2.2, and CC3.2.3.		
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including Senior Management and the Board of Directors, as appropriate.	CC2.1.1 CC3.2.2 CC3.2.3	See CC2.1.1, CC3.2.2, and CC3.2.3.		
CC5.0	CONTROL ACTIVITIES				
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.1	The Company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Company's security policies and review history to verify that the Company's security policies and procedures were documented and reviewed annually.	No exceptions noted.
		CC2.1.1 CC3.1.1 CC3.1.2 CC3.2.2	See CC2.1.1, CC3.1.1, CC3.1.2, and CC3.2.2.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.2.1	The Company's Access Control Policy documents the requirements for the following access control functions: <ul style="list-style-type: none"> ◇ Adding new users; ◇ Modifying users; and/or ◇ Removing an existing user's access. 	Inspected the Network Access and Authentication Policy, the completed onboarding and offboarding checklist for a sample of new hires, new contractors, offboarded employees, and offboarded contractors to verify that the Company's Access Control Policy documented the requirements for access control functions, including adding new users, modifying users, and removing existing users' access.	No exceptions noted.
		CC5.2.2	The Company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to verify that the Company had a formal systems development life cycle methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
		CC2.1.1 CC3.2.2 CC5.1.1	See CC2.1.1, CC3.2.2, and CC5.1.1.		
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC5.3.1	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 completed ticket for a sample of infrastructure and software changes to verify that the Company required 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.
		CC5.3.2	The Company's Operations Security Policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy, data backup schedule, and completed backup jobs to verify that the Company's Operations Security Policy documented requirements for backup and recovery of customer data.	No exceptions noted.
		CC5.3.3	The Company has formal retention and disposal procedures in place to guide the secure retention and disposal of Company and customer data.	Inspected the Confidential Data Policy and the data deletion records from the system to verify that the Company had formal retention and disposal procedures in place to guide the secure retention and disposal of Company and customer data. Inquired of the VP of IT to verify that there were no requests for customer data deletion.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
		CC1.3.3 CC2.2.1 CC3.1.1 CC3.1.2 CC3.2.3 CC5.1.1 CC5.2.1 CC5.2.2	See CC1.3.3, CC2.2.1, CC3.1.1, CC3.1.2, CC3.2.3, CC5.1.1, CC5.2.1, and CC5.2.2.		
CC6.0	LOGICAL AND PHYSICAL SECURITY				
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.1	The Company restricts privileged access to the application to authorized users with a business need.	Inspected the system-generated report of users with access to the production application to verify that the Company restricted privileged access to the application to authorized users with a business need.	No exceptions noted.
		CC6.1.2	The Company restricts privileged access to databases to authorized users with a business need.	Inspected the system-generated report of users with access to the production database to verify that the Company restricted privileged access to the databases to authorized users with a business need.	No exceptions noted.
		CC6.1.3	The Company restricts privileged access to the OS to authorized users with a business need.	Inspected the system-generated report of users with access to the production OS to verify that the Company restricted privileged access to the OS to authorized users with a business need.	No exceptions noted.
		CC6.1.4	The Company restricts privileged access to the production network to authorized users with a business need.	Inspected the system-generated report of users with access to the production network to verify that the Company restricted privileged access to the production network to authorized users with a business need.	No exceptions noted.
		CC6.1.5	The Company restricts access to migrate changes to production to authorized personnel.	Inspected the system-generated report of users with access to migrate changes to production environment to verify that the Company restricted access to migrate changes to production to authorized personnel.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.1.6	The Company maintains a formal inventory of production system assets.	Inspected the asset inventory to verify that the Company maintained a formal inventory of production system assets.	No exceptions noted.
		CC6.1.7	The Company requires authentication to systems and applications to use unique username and password.	Inspected the authentication process to key systems and applications to verify that the Company required authentication to systems and applications to use unique username and password.	No exceptions noted.
		CC5.2.1	See CC5.2.1.		
		CC6.2.1	The Company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the completed offboarding checklist for a sample of offboarded employees and offboarded contractors to verify that the Company completed termination checklists to ensure that access was revoked for terminated employees within SLAs.	No exceptions noted.
		CC6.2.2	The Company ensures that user access to in-scope system components is based on job role and function.	Inspected the Network Access and Authentication Policy and the report of systems that access was provisioned to for a sample of new hires and new contractors to verify that user access to in-scope system components was based on job role and function.	No exceptions noted.
		CC5.2.1 CC6.1.1 CC6.1.2 CC6.1.3 CC6.1.4 CC6.1.5	See CC5.2.1, CC6.1.1, CC6.1.2, CC6.1.3, CC6.1.4, and CC6.1.5.		

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
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.	CC5.2.1 CC6.1.1 CC6.1.2 CC6.1.3 CC6.1.4 CC6.1.5 CC6.2.1 CC6.2.2	See CC5.2.1, CC6.1.1, CC6.1.2, CC6.1.3, CC6.1.4, CC6.1.5, CC6.2.1, and CC6.2.2.		
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.4.1	Physical security is the responsibility of subservice organizations (refer to Section 3 for the subservice organization control activities).		
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	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.	Inspected the Retention Policy and Media, Data Destruction, Sanitization Policy to verify that the Company would have electronic media containing confidential information purged or destroyed in accordance with best practices. Inquired of the VP of IT to verify that no confidential data was destroyed.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.5.2	The Company deactivates and revokes access to the application environment containing confidential information, in accordance with best practices, when customers leave the service.	Inspected the Confidential Data Policy and completed termination ticket for a sample of terminated customers to verify that the Company deactivated and revoked access to the application environment containing confidential information, in accordance with best practices, when customers left the service.	No exceptions noted.
		CC5.3.3 CC6.2.1	CC5.3.3 and CC6.2.1.		
		CC6.6.1	The Company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the results of the Qualys SSL server scan to verify that the Company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
		CC6.6.2	The Company uses an intrusion prevention system to provide continuous monitoring of the Company's network and early detection of potential security breaches.	Inspected the IPS configuration to verify that the Company used an intrusion prevention system to provide continuous monitoring of the Company's network and early detection of potential security breaches.	No exceptions noted.
		CC6.6.3	The Company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall rules to verify that the Company used firewalls and configured them to prevent unauthorized access.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.6.4	The Company has a patch management process in place to identify vulnerabilities to help ensure that workstations supporting the service are hardened against security threats.	Inspected the workstation patch compliance status and patch history for a sample of employee workstations to verify that a patch management process was in place to identify vulnerabilities to help ensure workstations supporting the service were hardened against security threats.	No exceptions noted.
		CC6.7.1	The Company encrypts portable devices when used.	Inspected the HD encryption settings for a sample of employee workstations to verify that Company issued workstations were equipped with encrypted hard drives.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC6.7.2	The Company has an MDM system in place to centrally manage mobile devices supporting the service.	Inspected the security policies enforced by the MDM system for a sample of employee workstations to verify that the Company had an MDM system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
		CC6.6.1	See CC6.6.1.		
		CC6.8.1	The Company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on relevant systems.	Inspected the security policies enforced by the MDM system for a sample of employee workstations and antivirus status on production servers to verify that anti-malware technology was deployed to environments commonly susceptible to malicious attacks.	No exceptions noted.
		CC6.6.2 CC6.6.3 CC6.6.4 CC6.7.2	See CC6.6.2, CC6.6.3, CC6.6.4, and CC6.7.2.		
CC7.0	SYSTEM OPERATIONS				
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.1	The Company's formal policies outline the requirements for the following functions related to IT / Engineering: <ul style="list-style-type: none">◇ Vulnerability management;◇ System monitoring.	Inspected the Operations Security Policy to verify that the Company's formal policies outlined the requirements for functions related to IT/Engineering, including vulnerability management and system monitoring.	No exceptions noted.
		CC7.1.2	Company-issued workstations are monitored by an MDM that scans for vulnerabilities, and identified vulnerabilities are tracked until remediation.	Inspected the MDM installed on employee workstations for a sample of active employees to verify that Company-issued workstations were monitored by an MDM that scans for vulnerabilities. Inquired of the VP of IT to verify that there were no vulnerabilities identified that resulted in remediation.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
		CC7.1.3	The Company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy and review history to verify that the Company's network and system hardening standards were documented, based on industry's best practices, and reviewed at least annually.	No exceptions noted.
		CC7.1.4	The Company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy and configuration management tool to verify that the Company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	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.	CC2.1.2 CC6.6.2 CC6.6.4 CC7.1.1 CC7.1.2	See CC2.1.2, CC6.6.2, CC6.6.4, CC7.1.1, and CC7.1.2.		
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.1	The Company's security 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.	Inspected the Incident Response Policy to verify that the Company's security incidents were to be 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 VP of IT to verify that there were no security incidents reported.	Non-Occurrence noted. Pease Bell was unable to opine on the operating effectiveness of this control activity as there were no confirmed security incidents reported during the examination period.
		CC2.2.1	See CC2.2.1		

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC7.4.1	The Company tests their incident response plan at least annually.	Inspected the fire drill test results to verify that the Company tested their Incident Response Plan annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC2.2.1 CC7.3.1	See CC2.2.1 and CC7.3.1.		
		CC2.2.1 CC3.2.1 CC7.3.1 CC7.4.1	See CC2.2.1, CC3.2.1, CC7.3.1, and CC7.4.1.		
CC8.0	CHANGE MANAGEMENT				
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC5.2.2 CC5.3.1 CC6.1.5	See CC5.2.2, CC5.3.1, and CC6.1.5.		
CC9.0	RISK MITIGATION				
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.1	The Company has a Disaster Recovery/Business Continuity Plan in place that outlines communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Disaster Recovery/Business Continuity Plan to verify that the Company had a Disaster Recovery/Business Continuity Plan in place that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
		CC9.1.2	The Company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the Cyber Insurance Policy to verify that the Company maintained cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.

Criteria #	Criteria	Control #	Controls Specified by the Company	Test of Operating Effectiveness	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC3.1.2 CC3.2.2	See CC3.1.2 and CC3.2.2.		
		CC2.3.4 CC3.1.2 CC3.2.3	See CC2.3.4, CC3.1.2, and CC3.2.3.		