PRESCIENT
ASSURANCE

July 24, 2025

Prescient Assurance LLC
1900 Church Street, Suite 300
Nashville, TN 37203

In connection with your engagement to report on Dart Health Technology LLC's (service organization) description of its system titled Data Nexus System Description throughout the period April 12, 2025 to July 11, 2025 (description) based on the criteria set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria) and the suitability of the design and operating effectiveness of the controls included in the description throughout the period April 12, 2025 to July 11, 2025 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security, Confidentiality and Availability" set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented throughout the period observation period in accordance with the description criteria and whether the controls stated in the description were suitably designed and operating effectively throughout the period April 12, 2025 to July 11, 2025 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We confirm, to the best of our knowledge and belief, as of July 24, 2025, the date of your report, the following representations made to you during your examination:

1) We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

2) We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.

3) We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

4) We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.

5) We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls included in the description.

6) We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.

7) We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.

8) We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.

9) We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.

10) We are responsible for designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.

11) We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.

12) We have provided you with the following:

    a) All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.

    b) Access to additional information you have requested from us for the purpose of the engagement.

    c) Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.

13) We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

14) We have disclosed to you any known events subsequent to the period covered by the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design or operating effectiveness of the controls, or our assertion.

15) We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.

16) We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization’s system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.

17) We also have disclosed to you all instances about which we are aware of the following:

    a) Misstatements and omissions in the description.

    b) Instances in which controls have not been suitably designed or implemented as described.

    c) Instances in which controls did not operate effectively or as described.

18) We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements throughout the period April 12, 2025 to July 11, 2025.

19) We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.

20) We have disclosed to you the effects of the COVID-19 pandemic on Dart Health Technology LLC, its operations, and technologies used in providing services.

21) We have disclosed to you any communications to customers and business partners about changes in our service level agreements or commitments as a result of the COVID-19 pandemic.

22) We have responded fully to all inquiries made to us by you during the examination.

23) We understand that your report is intended solely for the use and information of management of the service organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information, if any. We intend to distribute your report only to those specified parties.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

Signed by:
Brian Sage
F3B995D2F40D400...

Name

CEO

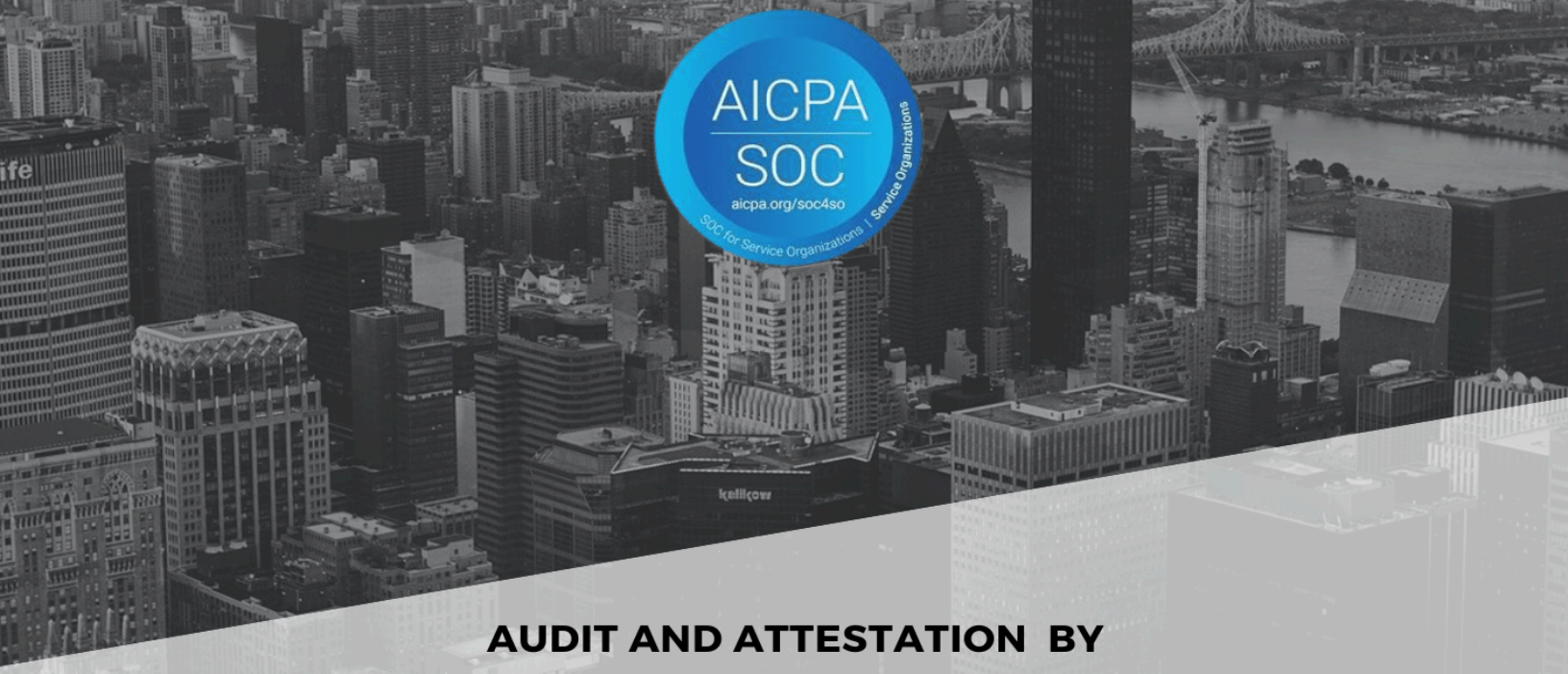
Title

SOC 2 Type 2 Report

Dart Health Technology LLC

April 12, 2025 to July 11, 2025

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Confidentiality and Availability



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

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

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



AICPA NOTICE:

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

Table of Contents

Management's Assertion 6
INDEPENDENT SERVICE AUDITOR'S REPORT 9
Scope 9
Service Organization's Responsibilities 9
Service Auditors' Responsibilities 10
Inherent Limitations 11
Opinion 11
Restricted Use 11
SYSTEM DESCRIPTION 13
DC 1: Company Overview and Types of Products and Services Provided 14
DC 2: The Principal Service Commitments and System Requirements 14
DC 3: The Components of the System Used to Provide the Services 15
3.1 Infrastructure 16
3.2 Software 16
3.3 People 18
3.4 Data 18
3.5 Processes and procedures 19
3.6 Change management 20
3.7 Boundaries of the system 21
DC 4: Disclosures About Identified Security Incidents 21
DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved 22
5.1 Integrity and ethical values 22
5.2 Commitment to competence 22
5.3 Management's philosophy and operating style 23
5.4 Organizational structure and assignment of authority and responsibility 23
5.5 HR policies and practices 24
5.6 Risk assessment process 24
5.7 Integration with risk assessment 24
5.8 Information and communication systems 24
5.9 Monitoring controls 25
5.9.1 On-going monitoring 25
5.10 Reporting deficiencies 25
DC 6: Complementary User Entity Controls (CUECs) 25
DC 7: Complementary Subservice Organization Controls (CSOCs) 26

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant 27
DC 9: Disclosures Of Significant Changes In Last 1 Year 28
Tests of Operating Effectiveness and Results of Tests 30
Scope of Testing 30
Types of Tests Generally Performed 30
General Sampling Methodology 31
Reliability of Information Provided by the Service Organization 31
Test Results 32

SECTION 1

Management's Assertion



Management's Assertion

We have prepared the accompanying description of Dart Health Technology LLC's system throughout the period April 12, 2025 to July 11, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Dart Health Technology LLC's system that may be useful when assessing the risks arising from interactions with Dart Health Technology LLC's system, particularly information about system controls that Dart Health Technology LLC 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, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

a. The description presents Dart Health Technology LLC's system that was designed and implemented throughout the period April 12, 2025 to July 11, 2025 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 12, 2025 to July 11, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Dart Health Technology LLC's controls during that period.
c. The controls stated in the description operated effectively throughout the period April 12, 2025, to July 11, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Dart Health Technology LLC's controls operated effectively throughout the period.

Signed by:
Brian Sage
F3B995D2F40D400...

Brian Sage
CEO
Dart Health Technology LLC

SECTION 2

Independent Service Auditor's Report



INDEPENDENT SERVICE AUDITOR'S REPORT

To: Dart Health Technology LLC

Scope

We have examined Dart Health Technology LLC's ("Dart Health Technology LLC") accompanying description of its Data Nexus system found in Section 3, titled Dart Health Technology LLC System Description throughout the period April 12, 2025, to July 11, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 12, 2025, to July 11, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

Service Organization's Responsibilities

Dart Health Technology LLC 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 Dart Health Technology LLC's service commitments and system requirements were achieved. In Section 1, Dart Health Technology LLC has provided the accompanying assertion titled "Management's Assertion of Dart Health Technology LLC" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Dart Health Technology LLC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered

by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

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

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.

2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.

3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.

4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

5. Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

6. Evaluating the overall presentation of the description.

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

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

Inherent Limitations

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

Opinion

In our opinion, in all material respects:

a. The description presents Dart Health Technology LLC's system that was designed and implemented throughout the period April 12, 2025, to July 11, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 12, 2025, to July 11, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Dart Health Technology LLC's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period April 12, 2025, to July 11, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Dart Health Technology LLC's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Dart Health Technology LLC, user entities of Dart Health Technology LLC's system during some or all of the period April 12, 2025 to July 11, 2025, business partners of Dart Health Technology LLC subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.

2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.

3. Internal control and its limitations.

4. Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.

6. The applicable trust services criteria.

7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

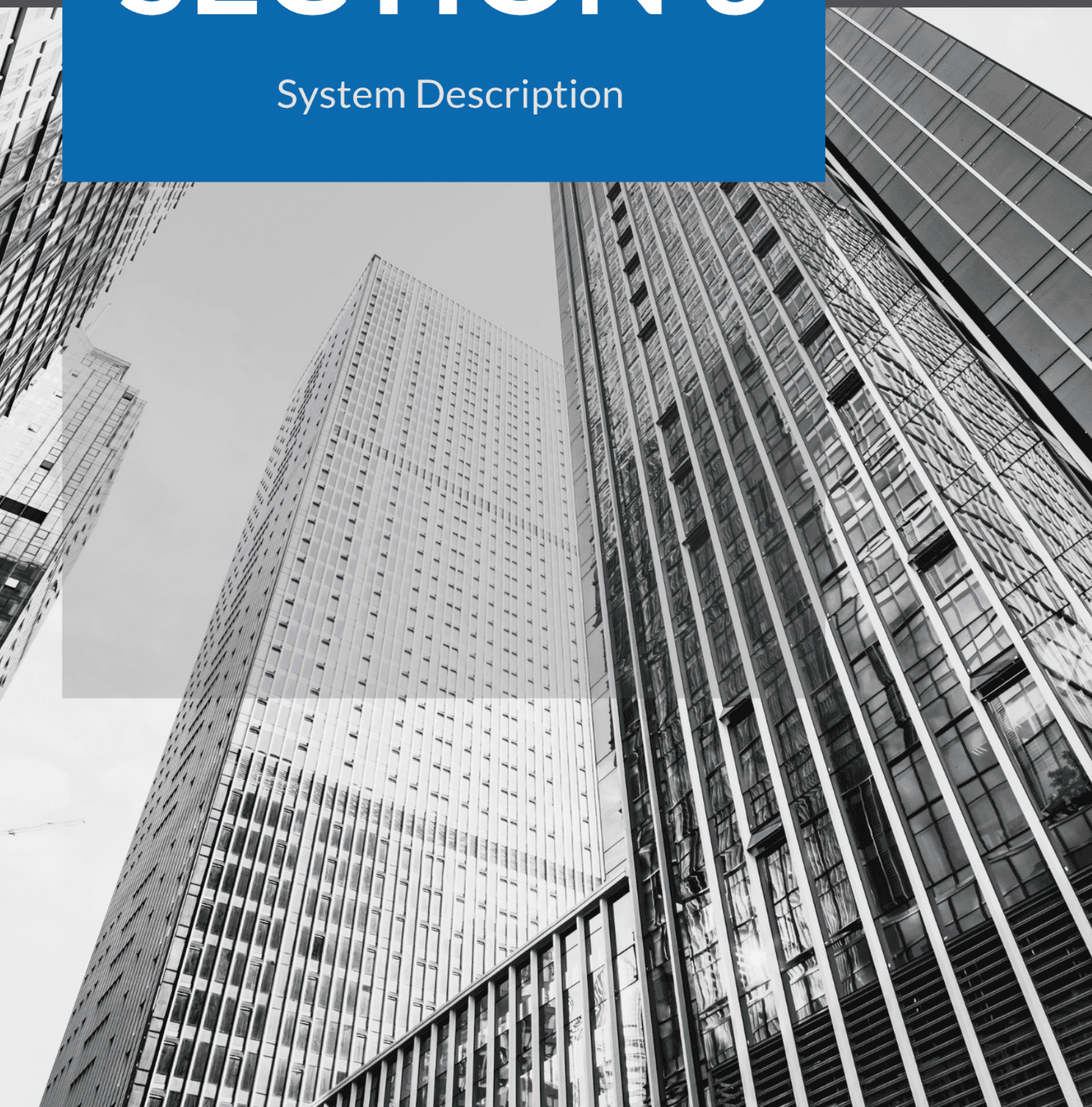
This report is not intended to be, and should not be, used by anyone other than these specified parties.

Signed by:
Prescient Assurance
0056D487564F4AE...

Prescient Assurance LLC
July 24, 2025

SECTION 3

System Description



DC 1: Company Overview and Types of Products and Services Provided

Company Background

Dart Health Technology LLC (the "company") was founded on 07/06/2022 by Brian Sage and Jason Cole to provide data ETL and storage services to healthcare benefits administration entities. The organization is based out of Centennial, Colorado with additional sites in Englewood, Colorado.

Description of services overview or services provided

The company's core product, the Data Nexus (the "system") is a Software as a Service (SaaS) solution that includes the following services:

- Secure reception and transmission of employee benefits, eligibility, enrollment, and benefits utilization data — enables the company's customers to not have to re-invent the wheel when faced by the same challenges besetting the healthcare benefits administration industry, giving our customers their resources and time back to invest in their core business
- Several secure transmission standards, including SFTP, and web-accessible, authenticated API — enables the company's customers to utilize our highly-available service instead of having to configure and maintain the same on their own
- Configurable data output standards — enables the company's customers to receive their customers data sooner, creating shorter timelines, fewer errors, and happier customers

DC 2: The Principal Service Commitments and System Requirements

The company designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that the company makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that the company has established for the services. Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;

- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Disaster recovery procedures

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements and trainings with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between the company and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

DC 3: The Components of the System Used to Provide the Services

The System description is comprised of the following components:

- **Infrastructure** – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- **Software** - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

- **People** - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data** – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedures** – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

3.1 Primary Infrastructure

The company maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner.

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Cloud Hosting Services	Virtual Private Cloud (VPC) environment that protects the network from unauthorized external access.
GitHub	Codebase	Maintain code commit discipline, ability to perform rollbacks, and CI/CD pipeline performance
Shortcut	Communication Service	Maintain operational workflow discipline

3.2 Primary Software and Applications

The company is responsible for managing the development and operation of the Data Nexus platform including infrastructure components such as servers, databases, and storage systems. The company's in-scope infrastructure and software components are shown in the table below:

System/Application	Operating System	Purpose
AWS Transfer Family	AWS	Simplifies secure file transfers to and from Amazon S3 or Amazon EFS using SFTP, FTPS, and FTP
Route53	AWS	Highly available and scalable Domain Name System (DNS) web service designed to route users to internet applications by translating domain names into their corresponding IP addresses.
S3	AWS	Object storage service designed to securely encrypt, store, and retrieve any amount of cloud-accessible data
EC2	AWS	Provides resizable cloud compute capacity, including virtual servers, leased servers, static IP management and leasing, and elastic load balancers
HTTPS certificate manager	AWS	Provisioning and deployment tools to manage SSL/TLS certificates used to secure applications and data in transit
Simple Queueing Service	AWS	Fully-managed messaging queue service to send, store, and receive messages between distributed software components
Secrets Manager	AWS	Provides for the rotation, management, and retrieval of credentials, API keys, and other secrets to enhance security
CloudWatch	AWS	Monitoring and observability service that collects and tracks metrics, logs, and events from AWS resources and applications, enabling real-time insights and proactive responses to operational events
IAM	AWS	Identity and Access Management (IAM) provides secure access control for AWS resources by enabling the creation and management of users, groups, roles, and permissions
RDS	AWS	Managed service for setting up, operating, and scaling relational databases in the cloud

ECS	AWS	Container orchestration service for running our proprietary containerized applications in the cloud

3.3 People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

The company has a staff organized in the following functional areas:

Management - Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

CEO - Brian Sage

CTO - Jason Cole

Operations - Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology - Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development - Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

3.4 Data

Data is categorized in four major types of data used by the company

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for the company	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences

Customer data	Information received from customers for processing or storage by the company. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by the company to operate the business. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, the company has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.5 Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by the CEO or the manager of the area in question. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

3.5.1 Physical security

The company's production servers are maintained by Amazon Web Services. The physical and environmental security protections are the responsibility of Amazon Web Services. The company reviews the attestation reports and performs a risk analysis of Amazon Web Services on at least an annual basis.

3.5.2 Logical access

The company provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems are split into three levels; Administrator, User, and No Access. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing the company's policies, completing security training.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 24 business hours for that employee's termination.

3.5.3 Computer operations - backups

Customer data is backed up and monitored by the customer's assigned engineering lead for completion and exceptions. If there is an exception, the customer's assigned engineering lead performs or assigns troubleshooting tasks to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in declarative configurations according to the policies. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer operations - availability

The company maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

The company internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

The company utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

3.5.5 Change management

The company maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

3.5.6 Data communications

The company has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the company application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The company engages a SaaS vulnerability scanning service to perform ongoing scans and an external security firm to perform annual vulnerability scans and penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

3.7 Boundaries of the system

The boundaries of the Data Nexus system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Data Nexus system.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

DC 4: Disclosures About Identified Security Incidents

No significant incidents have occurred to the services provided to user entities.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

5.1 Integrity and ethical values

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 company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the company's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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 and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.
- The company requires contractors to sign a confidentiality agreement at the time of engagement.
- The company performs background checks on new employees.

5.2 Commitment to competence

The company's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

5.3 Management's philosophy and operating style

The company management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way the company can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require the company to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- The company's executive leadership, or a relevant subcommittee, is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risks. The executive leadership provides feedback and direction to management as needed.
- The company's executive leadership has documented guidance outlining its oversight responsibilities for internal controls.

5.4 Organizational structure and assignment of authority and responsibility

The company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The company's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring 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.

Specific control activities that the service organization has implemented in this area are described below:

- The company maintains an organizational chart that describes the organizational structure and reporting lines.

5.5 HR policies and practices

The company's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. The company's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires employees to sign a confidentiality agreement during onboarding.
- The company managers are required to complete performance evaluations for direct reports at least annually.
- The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

5.6 Risk assessment process

The company's risk assessment process identifies and manages risks that could potentially affect the company's ability to provide reliable and secure services to our customers. As part of this process, the company maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular company product development process so they can be dealt with predictably and iteratively.

5.7 Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of the company's system; as well as the nature of the components of the system result in risks that the criteria will not be met. The company addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, the company's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and communication systems

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

The company uses several information and communication channels internally to share information with management, employees, contractors, and customers. The company uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools.

5.9 Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. The company's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

5.9.1 On-going monitoring

The company's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in the company's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of the company's personnel.

5.10 Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

DC 6: Complementary User Entity Controls (CUECs)

The company's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to the company's services to be solely achieved by the company control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of the company's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met.

1. User entities are responsible for understanding and complying with their contractual obligations to the company.

2. User entities are responsible for notifying the company of changes made to technical or administrative contact information.

3. User entities are responsible for maintaining their own system(s) of record.

4. User entities are responsible for ensuring the supervision, management, and control of the use of the company services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the company services.

6. User entities are responsible for providing the company with a list of approvers for security and system configuration changes for data transmission.

7. User entities are responsible for immediately notifying the company of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

DC 7: Complementary Subservice Organization Controls (CSOCs)

The company's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to the company's services to be solely achieved by the company control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of the company.

The following subservice organization controls are assumed to be implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
Security	CC6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC6.4	Access to server locations is managed by electronic access control devices.
Security	CC7.2	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
Security	CC7.2	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
Availability	A1.2	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.

Availability	A1.2	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.

The company management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, the company performs monitoring of the subservice organization controls, including the following procedures

- Reviewing and reconciling security reports
- Holding periodic discussions with vendors and subservice organization(s)
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

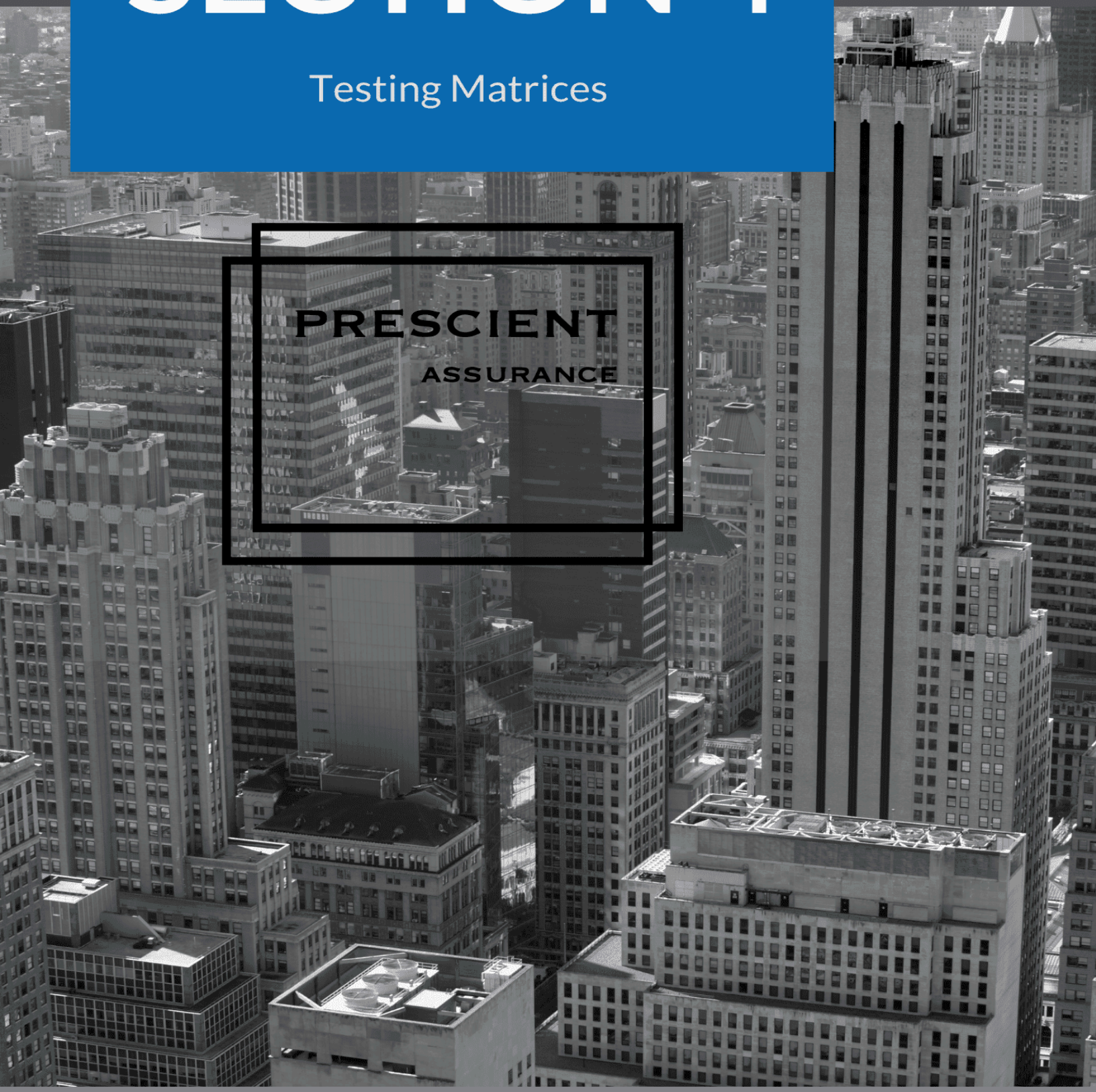
All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to the company's Data Nexus system.

DC 9: Disclosures Of Significant Changes In Last 1 Year

No significant changes occurred during this period.

SECTION 4

Testing Matrices



Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Data Nexus provided by Dart Health Technology LLC. The scope of the testing was restricted to Data Nexus, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period April 12, 2025 to July 11, 2025.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	**Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.**

Inspection	**Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following:** • **Examination / Inspection of source documentation and authorizations to verify transactions processed.** • **Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.** • **Examination / Inspection of systems documentation, configurations, and settings; and** • **Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.**
Observation	**Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.**
Re-performance	**Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.**

General Sampling Methodology

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

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

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected company evaluations to determine that the company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	No exceptions noted.
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring configurations to determine that an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that the company's data backup policy documents requirements for backup and recovery of customer data.	No exceptions noted.

A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	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 company's risk register to determine that 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.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	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 to determine that the company had 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.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the intrusion detection system configurations to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that the company's data backup policy documents requirements for backup and recovery of customer data.	No exceptions noted.

C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that the company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that the company had formal retention and disposal procedures to guide the secure retention and disposal of company and customer data.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	Inspected the data management policy to determine that the company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	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 written agreements for a sample of vendors and determined that the company had written agreements in place with vendors and related third-parties and that these agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.

C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected data management policy to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. Inquired with the company that no customer data containing confidential information from the application environment was deleted during the audit window.	Not tested, Control activity did not operate during the period.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company performs background checks on new employees. Inspected the personnel records to determine that no new employees were hired during the audit period.	Not tested, Control activity did not operate during the period.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the personnel records to determine that no new employees were hired during the audit period. Inspected the Human Resource Security Policy and code of conduct policy to determine that employees who violate information security policies may face disciplinary consequences in proportion to their violation.	Not tested, Control activity did not operate during the period.

CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evaluations for a sample of current employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the Human Resource Security Policy to determine that the company requires employees to sign a confidentiality agreement during onboarding. Inspected the personnel records to determine that no new employees were hired during the audit period.	Not tested, Control activity did not operate during the period.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the Human Resource Security Policy to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement. Inspected the personnel records to determine that no new contractors were hired during the audit period.	Not tested, Control activity did not operate during the period.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Code of Conduct to determine that all contractors are required to comply with its terms in all business matters. Inspected the personnel list to determine that no contractors were engaged during the audit window.	Not tested, Control activity did not operate during the period.

CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership meets at least annually and maintains formal meeting minutes.	Inspected the executive meeting minutes to determine that the company's executive leadership meets at least annually and maintains formal meeting minutes.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership, or a relevant subcommittee, is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risks. The executive leadership provides feedback and direction to management as needed.	Inspected the meeting minutes to determine that the company's executive leadership or a relevant subcommittee was briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The executive leadership provides feedback and direction to management as needed.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership has documented guidance outlining its oversight responsibilities for internal controls.	Inspected the documented Information Security Roles and Responsibilities and Ethical management Survey to determine that the company's executive leadership has defined oversight responsibilities for internal controls.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership has sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The executive leadership engages third-party information security experts and consultants as needed.	Inspected the profiles of the company's executive leadership to determine that they possess sufficient expertise to oversee management's ability to design, implement, and operate information security controls. Inspected the Penetration Test Report to determine that executive leadership engages third-party information security experts and consultants as needed.	No exceptions noted.

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected company's chart to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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 determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's executive leadership has documented guidance outlining its oversight responsibilities for internal controls.	Inspected the documented Information Security Roles and Responsibilities and Ethical management Survey to determine that the company's executive leadership has defined oversight responsibilities for internal controls.	No exceptions noted.

CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the personnel records to determine that no new employees were hired during the audit period. Inspected security awareness training records of current employees to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company performs background checks on new employees. Inspected the personnel records to determine that no new employees were hired during the audit period.	Not tested, Control activity did not operate during the period.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evaluations for a sample of current employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.

CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the personnel records to determine that no new employees were hired during the audit period. Inspected the Human Resource Security Policy and code of conduct policy to determine that employees who violate information security policies may face disciplinary consequences in proportion to their violation.	Not tested, Control activity did not operate during the period.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evaluations for a sample of current employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.

CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs 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. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment dashboard that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected product documentation to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan and the Policy acknowledgements to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the personnel records to determine that no new employees were hired during the audit period. Inspected security awareness training records of current employees to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized internal users.	Inspected internal communication channel to determine that the company communicates system changes to authorized internal users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the Information security policy and the anonymous whistleblower form that the company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements for a sample of vendors and determine that the company had written agreements in place with vendors and related third-parties and that these agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the technical support resources to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the Terms and Conditions to determine that the company's security commitments are communicated to customers in SaaS Agreement or Terms of Service (TOS).	No exceptions noted.

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company 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 external-facing support system to determine that 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.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected product documentation to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	inspected the policy to determine that the company notifies customers of critical system changes that may affect their processing. Inquired with the company that they did not make any critical system changes that effected their customers processing during the period.	Not tested, Control activity did not operate during the period.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	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 to determine that the company had 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.	No exceptions noted.

CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment report to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a 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 to determine that the company had 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.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company'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 company's risk register to determine that 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.	No exceptions noted.

CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and annual disaster recovery tabletop exercise to determine that the company had a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and compliance reports to determine that the company had a vendor management program in place that included a critical third-party vendor inventory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 to determine that the company had 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.	No exceptions noted.

CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 company's risk register to determine that 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.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected configuration evidence to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities per SLAs.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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 to determine that the company had 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.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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 company's risk register to determine that 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.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and compliance reports to determine that the company had a vendor management program in place that included a critical third-party vendor inventory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.

CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company 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. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment dashboard that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities per SLAs.	No exceptions noted.

CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control self-assessment dashboard that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and compliance reports to determine that the company had a vendor management program in place that included a critical third-party vendor inventory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company 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 to determine that the company had 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.	No exceptions noted.

CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy, which includes access provisioning, de-provisioning, access change, and review procedures to determine that the company has established access control procedures.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (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, which includes change control for system updates, version control, and secure testing, to determine that it effectively governs system development and maintenance practices.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan and the Policy acknowledgements to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that the company's data backup policy documents requirements for backup and recovery of customer data.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (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, which includes change control for system updates, version control, and secure testing, to determine that it effectively governs system development and maintenance practices.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that the company had formal retention and disposal procedures to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the information security policies and procedures to determine that the company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a 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 to determine that the company had 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.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and compliance reports to determine that the company had a vendor management program in place that included a critical third-party vendor inventory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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 to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment report to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company's datastores housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected access channel to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the user listings to determine that the company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected GitHub user listings to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Inspected the asset inventory to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Inspected user listings to determine that the company restricts privileged access to databases to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected user listings to determine that the company restricts privileged access to the operating system to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected user listings to determine that the company restricts privileged access to the production network to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected evidence that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the user listings to determine that the company restricts privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	System access restricted to authorized access only	Inspected user listings to determine that the company's system access is restricted to authorized users only.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that the company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy, which includes access provisioning, de-provisioning, access change, and review procedures to determine that the company has established access control procedures.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected evidence to determine that the company requires passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the user listings to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected encryption certificate to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected subnet configurations to determine that the company's network is segmented to prevent unauthorized access to customer data.	No exceptions noted.

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy, which includes access provisioning, de-provisioning, access change, and review procedures to determine that the company has established access control procedures.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected access reviews to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the access rights of all users to ensure they are promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours. Inspected the People section on the compliance platform to determine that no employees were terminated during the audit period.	Not tested, Control activity did not operate during the period.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected evidence that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected evidence that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected access reviews to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the access rights of all users to ensure they are promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours. Inspected the People section on the compliance platform to determine that no employees were terminated during the audit period.	Not tested, Control activity did not operate during the period.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy, which includes access provisioning, de-provisioning, access change, and review procedures to determine that the company has established access control procedures.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected evidence that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected access reviews to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inquired with the company that they had no electronic media containing confidential information that was purged or destroyed during the window.	No exceptions noted.

CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected data management policy to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. Inquired with the company that no customer data containing confidential information from the application environment was deleted during the audit window.	Not tested, control did not operate during the audit period.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that the company had formal retention and disposal procedures to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the access rights of all users to ensure they are promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours. Inspected the People section on the compliance platform to determine that no employees were terminated during the audit period.	Not tested, control did not operate during the audit period.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected encryption certificate to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall review to determine that the company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall configurations to determine that the company uses firewalls and configures them to prevent unauthorized access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the operations security policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability results and evidence of remediation of identified vulnerabilities to determine that the company had infrastructure supporting the service patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the intrusion detection system configurations to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the user listings to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the user listings to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.

CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Inspected device encryption data to determine that the company encrypts portable and removable media devices when used. Inquired with the company that they do not use removable media in their business.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the MDM configurations to determine that the company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability results and evidence of remediation of identified vulnerabilities to determine that the company had infrastructure supporting the service patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (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, which includes change control for system updates, version control, and secure testing, to determine that it effectively governs system development and maintenance practices.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the anti-malware deployment for a sample of current employee workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configures them to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected configuration evidence to determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the policy files to determine that the company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	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 company's risk register to determine that 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.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability results and evidence of remediation of identified vulnerabilities to determine that the company had infrastructure supporting the service patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the policy files to determine that the company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring configurations to determine that an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the intrusion detection system configurations to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities per SLAs.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inquired with the company to determine that no security or privacy incidents took place during the window.	Not tested, control did not operate during the audit period.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan and the Policy acknowledgements to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company tests their incident response plan at least annually.	Inspected the tabletop exercise report to determine that the company tests their incident response plan at least annually.	No exceptions noted.

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Inspected the tabletop exercise report to determine that the company tests their incident response plan at least annually.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan and the Policy acknowledgements to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability results and evidence of remediation of identified vulnerabilities to determine that the company had infrastructure supporting the service patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inquired with the company to determine that no security or privacy incidents took place during the window.	Not tested, control did not operate during the audit period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the tabletop exercise report to determine that the company tests their incident response plan at least annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inquired with the company to determine that no security or privacy incidents took place during the window.	Not tested, control did not operate during the audit period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan and annual disaster recovery tabletop exercise to determine that the company had a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	No exceptions noted.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan and the Policy acknowledgements to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected GitHub user listings to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the operations security policy to determine that the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has a formal systems development life cycle (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, which includes change control for system updates, version control, and secure testing, to determine that it effectively governs system development and maintenance practices.	No exceptions noted.

CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the vulnerability results and evidence of remediation of identified vulnerabilities to determine that the company had infrastructure supporting the service patched as a part of routine maintenance, and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration testing report to determine that the company's penetration testing was performed at least annually. Inspected evidence of remediation for identified vulnerabilities in the penetration report to determine that remediation plans are developed and changes are implemented to remediate vulnerabilities per SLAs.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of code changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 to determine that the company had 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.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 company's risk register to determine that 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.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the timestamped cybersecurity insurance policy document to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plans to determine that the company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and compliance reports to determine that the company had a vendor management program in place that included a critical third-party vendor inventory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements for a sample of vendors and determined that the company had written agreements in place with vendors and related third-parties and that these agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.