Faraday, Inc.
Burlington, Vermont

System and Organization Controls Report on the Description and Tests of Operating Effectiveness of the Faraday AI System

Controls Placed in Operation Relevant to Security, Availability, and Confidentiality

SOC 2® Type 2 Report

November 1, 2020 to October 31, 2021

WIPFLI

Faraday, Inc.

System and Organization Controls Report on the Description and Tests of Operating Effectiveness of the Faraday AI System

November 1, 2020 to October 31, 2021

Table of Contents

Section 1
Faraday, Inc.’s Assertion

Faraday, Inc.'s Assertion

We have prepared the accompanying description in Section 3 titled "Description of the Faraday AI System Provided by Faraday, Inc." (the "description") throughout the period November 1, 2020 to October 31, 2021, based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (*AICPA*, Description Criteria)*. The description is intended to provide report users with information about the Faraday AI System that may be useful when assessing the risks arising from interactions with Faraday, Inc.'s ("Faraday") system, particularly information about system controls that Faraday has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

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

1. The description presents the Faraday AI System that was designed and implemented throughout the period November 1, 2020 to October 31, 2021, in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Faraday's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Faraday's controls throughout that period.
3. The controls stated in the description operated effectively throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Faraday's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Faraday's controls operated effectively throughout that period.

Section 2
Independent Service Auditor's Report

WIPFLI

Independent Service Auditor's Report

Management of Faraday, Inc.
Burlington, Vermont

Scope

We have examined the accompanying description in Section 3 titled "Description of the Faraday AI System Provided by Faraday, Inc." throughout the period November 1, 2020 to October 31, 2021 (the "description"), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (the "description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Faraday, Inc.'s ("Faraday") service commitments and system requirements were achieved based on the trust services criteria related to security, availability, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Faraday uses multiple subservice organizations to provide cloud computing services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Faraday, to achieve Faraday's service commitments and system requirements based on the applicable trust services criteria. The description presents Faraday's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Faraday's controls. The description does not disclose the actual controls at the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Faraday 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 Faraday's service commitments and system requirements were achieved. Faraday has provided the accompanying assertion in Section 1 titled "Faraday, Inc.'s Assertion" (the "assertion") about the description and the suitability of the design and operating effectiveness of controls stated therein. Faraday 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.

Independent Service Auditor's Report (Continued)

Service Auditor's Responsibilities

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

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

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

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

Inherent Limitations

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

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

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

Independent Service Auditor's Report (Continued)

Description of Tests of Controls
The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 titled "Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results" of this report.

Opinion
In our opinion, in all material respects:

- The description presents the Faraday AI System that was designed and implemented throughout the period November 1, 2020 to October 31, 2021, in accordance with the description criteria.
- The controls stated in the description were suitably designed throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Faraday'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 organizations and user entities applied the complementary controls assumed in the design of Faraday's controls throughout that period.
- The controls stated in the description operated effectively throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that Faraday's service commitments and system requirements would be achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Faraday's controls operated effectively throughout that period.

Restricted Use
This report, including the description of the tests of controls and results thereof in Section 4, is intended solely for the information and use of Faraday, user entities of Faraday's Faraday AI System during some or all of the period November 1, 2020 to October 31, 2021, business partners of Faraday subject to risks arising from interactions with the Faraday AI System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators, all who have sufficient knowledge and understanding of the following:

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

Independent Service Auditor's Report (Continued)

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

Wipfli LLP

Wipfli LLP

South Portland, Maine
November 12, 2021

Section 3
Description of the Faraday AI System Provided by Faraday, Inc.

Description of the Faraday AI System Provided by Faraday, Inc.

Company Overview

Nature of Business

Faraday, Inc. ("Faraday" or the "Company") was organized as a Delaware corporation named Brighter Planet Technology Services, Inc., on December 10, 2012. The business of Faraday is to provide web-based software to optimize consumer-facing businesses using artificial intelligence (AI). Faraday is composed of an experienced management team with expertise in the application of machine learning (ML) principles to business objectives, as well as in the development of software. Faraday has been developing its software since formation. Faraday has headquarters located in Burlington, Vermont.

Principal Service Commitments and System Requirements

Faraday designs its processes and procedures related to the AI platform to meet its objectives for the successful delivery of services. Those objectives are based on the service commitments Faraday makes to user entities, the laws and regulations that govern the provision of these services, and the financial, operational, and compliance requirements Faraday has established for the services. The Faraday AI System is subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA), as well as state privacy security laws and regulations in the jurisdictions in which Faraday operates.

Security, confidentiality, and availability commitments to user entities are documented and communicated in service level agreements (SLA) and other client agreements, as well as in the description of the service offering provided online.

- Security commitments include principles within the fundamental designs of the AI platform that are designed to permit system users to access the information they need based on their roles in the system, while restricting them from accessing information not needed for their role.

- Confidentiality commitments include the use of encryption technologies to protect client data both at rest and in transit.

- Availability commitments include the ongoing monitoring and uptime of the platform.

Faraday establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Faraday's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the platform is designed and developed, the platform is operated, the internal business systems and networks are managed, and employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required when providing the AI Platform.

Description of the Faraday AI System

Critical Infrastructure

Faraday leverages third-party hosted infrastructure to host the Faraday AI System (app.faraday.io). The third party provides multizone redundancy, auto-scaling capabilities, and multi-region failovers. It provides physical security, environmental protection, and redundant infrastructure to Faraday. Faraday's Chief Information Security Officer (CISO) obtains and reviews the third party's System and Organization Controls (SOC) report to evaluate the internal control environment and the impact of exceptions noted for relevant controls.

Company Overview (Continued)

Description of the Faraday AI System (Continued)

Critical Infrastructure (Continued)

The Faraday AI System is accessed as a software-as-a-service (SaaS) offering. Users log in to the software over a hypertext transfer protocol secure (HTTPS) connection using their web browser. Authentication is managed by a third party.

Software

The Faraday AI System comprises applications developed and maintained by Faraday's in-house Software Engineering group. The Software Engineering group enhances and maintains these services to support the needs of Faraday's clients and end users.

People

Faraday's staff is primarily located in Burlington, Vermont, and is organized in the following functional areas:

Functional Area	Responsibilities
Senior Management	Primarily responsible for ensuring Faraday meets investors', clients', and employees' expectations.
Sales and Marketing	Primarily responsible for acquiring new clients.
Client Success	Primarily responsible for managing existing clients.
Data Science	Primarily responsible for prescribing the data science methodology implemented in the Faraday AI System. In addition, responsible for consulting with clients.
Product Management	Overall ownership of the product direction, development, and operations.
Platform	Faraday's engineering team, primarily responsible for maintaining and improving the Faraday AI System.

Procedures

Senior Management has developed and communicated organizational policies and procedures to employees and clients. Changes to these procedures are performed at least annually and authorized by Senior Management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Confidentiality and availability
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization of, changes to, and termination of information system access
- Monitoring of security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage

Company Overview (Continued)

Description of the Faraday AI System (Continued)

Procedures (Continued)

- Incident response
- Maintenance of restricted access to system configurations, superuser functionality, master, passwords, powerful utilities, and security devices (for example, firewalls)

Data

Data, as defined by Faraday, falls into one of the following classifications:

- Account metadata
- Private client data
- Shared consumer data

Account metadata refers to data entered by end users and their account managers during and following registration to configure the Faraday AI System for the client's use. Examples of account metadata include authorized user details (e.g., email address), external data system credentials, audience descriptors, client journeys, points of interest, and business outcome definitions.

Private client data refers to data maintained by the client that is copied from the client's external data systems to the Faraday AI System for further processing and storage. Examples of private client data include client lists, lead lists, transaction records, and email engagement data.

Shared consumer data refers to data licensed by Faraday from consumer data vendors whose primary business is to collect, refine, and package consumer data for downstream licensing to firms like Faraday. Examples of shared consumer data include demographic, financial, psychographic, property, and life event details of U.S. adult consumers.

Change Management

Application Changes

The responsibilities of the Platform team, led by product and technical managers, include technical design, coding, and unit testing of new and upgraded product features. There are multiple aspects of application development activities, including the design and implementation of architecture, infrastructure, tools, and products. Application requirements are defined by the product manager and approved by the technical managers.

The code is developed using the latest mix of web development software tools. Developers follow a comprehensive set of guidelines and best practices when authoring source code. Code reviews are conducted by peers and technical managers to help ensure compliance with requirements and best practices.

Changes to the software and bug resolution are managed via product management software. This enforces control over the change process for the application. There is a written policy for entering tasks for changes to the software and bugs for corrections to the software. Tasks are approved for implementation by product and technical managers only.

Company Overview (Continued)

Description of the Faraday AI System (Continued)

Change Management (Continued)

Application Changes (Continued)

Application source code is stored and managed via a formal source code version control process using source code management software that is described further in the Source Code Access section. Four environments are maintained and are physically and logically separated from each other: development and testing on developer machines, testing on a continuous integration (CI) server, testing in staging, and production. All but the first are hosted with a cloud hosting provider.

Production Changes

The production environment has been designed to optimize system performance while helping to ensure the best possible security protocols. The design of the security controls and the system performance reviews are done regularly by platform experts to help ensure Faraday is using best practices.

Changes coming from the review process could include reclassification of data, reassessment of risk and changes in incident response and recovery plans, and verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during regular change management meetings and/or through system alerts.

The cloud hosting provider helps ensure, as part of its service, that patches are made to the operating system. Technical managers check regularly to see whether there are updates to other software used in the production environment. Once identified, a schedule is set to apply the patches.

Changes to the preproduction and production environments are controlled via tickets to help ensure documentation and process control of those changes.

Control of Changes

The product and technical managers meet at least weekly to discuss the current status and prioritize tasks and defect fixes for implementation. Once the tasks and bugs have been scheduled, the product and technical managers are responsible for controlling and coordinating aspects of the development process until release.

There are frequent meetings on the development of Faraday software with the technical and product managers and the entire Platform team. These meetings generally occur at least once a week.

Each change completed by the Platform team is posted to source code management software, and testing releases are produced and put on a testing server to help ensure each task and defect fix has been correctly completed. Updates are approved and scheduled through the change control process.

Defect Tracking and Audit Trail

Defect tracking is done in the ticketing software. Defects can be entered into the ticketing software by any Faraday employee. Each defect is evaluated, assigned to a developer, and then reassigned to testing until the defect is successfully corrected. Detailed instructions describing how an authorized team member is to add defects to the ticketing software are maintained. These instructions are available to team members in a common folder accessible to those who require access.

The determination of priority of the defect can be suggested by the person creating the defect fix but ultimately is agreed to or amended by the product and technical managers.

Company Overview (Continued)

Description of the Faraday AI System (Continued)

Source Code Access

Software source code created in the development process is stored and controlled through an industry-standard source code version control system. The software source code includes source code produced by the Platform and Data Science teams.

Engineers retrieve copies of source code through the version control system. The system provides standard versioning mechanisms including file revision management, version labeling mechanisms, and file status indicators. The version control system has built-in reconciliation logic to help ensure application developers don't collide or lose essential changes upon check-in.

Testing of Changes

Engineers test code they produce. Technical managers perform code reviews. Product managers perform verifications.

Tasks created in ticketing must contain details for the verification of that change. That list is put together initially by the engineer assigned to the task.

For defects, the technical managers outline the steps to test, but these are generally the same steps used to re-create the bug to help ensure it is corrected.

In either case (tasks or defects), additional care is taken by the product and technical managers working with the assigned engineer(s) to identify the potential for collateral impacts that can be the unintended result of coding for new functionality or correcting bugs.

Prior to release, tests are run on a hosted server setup that is a mirror image, in material aspects, of the production system.

Software Release Process

The Platform team performs testing of Faraday's software products and custom development in an environment independent from developers and development activities. Specific activities include system testing, environment testing, regression testing, release acceptance testing, and development of automated testing tools.

The software release testing process focuses on determining that product quality levels are maintained with respect to operational characteristics, performance characteristics, and system reliability. These aspects are tested and monitored against supported environments (operating systems and machine configurations) and usage scenarios based on anticipated production scenarios.

The software release testing process is synchronized with other activities through the project management tool. The testing process is applied to product releases.

Software release testing follows standardized procedures to determine that the system conforms to quality control standards prior to release. Software release testing focuses primarily on testing complete data flow throughout integration points. This includes installation, environment, and data integrity testing.

Company Overview (Continued)

Description of the Faraday AI System (Continued)

Software Build Process

With the exception of localized developer builds for unit testing purposes, software modules are produced through an automated build process. It is this build process that creates production software modules for release to the hosted production environment. Source codes used in the build process are retrieved from the master source code archives.

Application builds are performed automatically as code changes pass tests on CI. During periods of heavy development activity, builds may be produced frequently. Builds are cataloged and archived.

Third-Party Service Providers

Faraday uses various third-party vendors to assist in running its business operation and IT platform.

- Trello – A cloud-based project management service.
- Rippling – A cloud-based human resource management system.
- Google Apps for Business – A cloud-based suite of services used primarily by Faraday for email communication and document creation.
- GitHub – A cloud-based source code management system used by Faraday as its primary source code repository and additionally for code review, automated testing, and other software life cycle functions.
- Amazon Web Services (AWS) – A cloud host Faraday uses for data storage (S3), scalable computer resources (ECS), and other infrastructural functions.
- Google Cloud – A cloud host Faraday uses for database functions (BigQuery).
- Stitch Data – An infrastructure service provider that manages synchronization of some client data systems external to the Faraday AI System.
- BigML – A cloud ML platform that Faraday uses to build and employ some ML models.
- Pipedrive – A cloud-based client relationship management (CRM) solution.
- Dashlane – A cloud-based password manager Faraday employees use.
- Auth0 – A cloud authentication and identity management platform used by the Faraday AI System to authorize user logins.
- Slack – A cloud-based collaboration tool used day to day for active collaboration and access to historical company knowledge.
- Citus Data – A cloud-based database management tool.
- Dropbox – A cloud-based file storage and collaboration platform.

Faraday solicits evidence of security audits from third-party systems employed to develop and maintain Faraday's system. If SOC 2 or equivalent reports are not available, the CISO and system owner review the information provided by the vendor and make a determination of the suitability of the vendor's controls and practices.

Description of the Faraday AI System Provided by Faraday, Inc.

Relevant Aspects of Internal Control

Control Environment

Faraday is committed to providing clients and employees with a business environment that promotes ethical values, competent and timely service delivery, and clear roles and responsibilities through organizational structure, policies and procedures, and delivery on commitments to the client.

Faraday cultivates this environment by encouraging control consciousness on the part of employees. This awareness starts with executive management's involvement in the creation and monitoring of policies and procedures. Sign-off by a member of Senior Management is required for the creation of new or updated policies and procedures. Policies and procedures are then disseminated through the various levels of the organization. Such a control environment influences the way Faraday's business activities are structured, objectives are established, and risks are assessed.

Information and Communication

To help align Faraday's strategic and tactical decision making with operating performance, management is committed to maintaining effective communication with personnel. Information comes from both inside and outside Faraday and is used to guide Faraday's strategic and tactical decision making as well as to measure performance. External communications originate from a number of sources, take on many forms (state and federal legislation, client interaction, etc.), and are distributed to a number of destinations. Faraday's management has focused on establishing multiple formats and channels of external communications to facilitate timely and appropriate communications. Faraday's management monitors internal and external communications on an ongoing basis to assess the effectiveness of these communications.

Risk Assessment

Faraday's risk assessment process is its identification, analysis, and management of risks relevant to the delivery of services and protection of the client's data. Faraday has placed into operation a risk assessment process to identify and manage risks that could affect its ability to provide reliable services to its clients and help ensure the protection of clients' data. This process requires management to identify significant risks inherent in the software development and operational environments outlined in this report.

This process has facilitated the identification of various risks inherent in Faraday's software development and operational environment and resulted in the development and implementation of reasonable measures for the ongoing management and mitigation of these findings. The risks considered by Faraday management on an ongoing basis include the following:

- New industry legislation and regulations
- Changes in its operating environment
- New or modified information systems
- New technology
- Processes involving partner organizations
- External systems
- New product development

Relevant Aspects of Internal Control (Continued)

Control Activities

Within Faraday's business environment, control activities include the policies and procedures that help ensure management directives are carried out. They help ensure necessary actions are taken to address risks for achievement of Faraday's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Faraday has implemented a series of management activities to measure and assess various processes involved in servicing its client base.

Board of Directors

The Board of Directors meets quarterly to discuss Company objectives, policies, and the current state of the Company. The Board of Directors provides oversight and recommendations to management to further help develop the company from an independent standpoint. Some of the Board of Directors' responsibilities are the business planning process and review of the ongoing risk assessment and management process and revision of these processes when necessary to support the achievement of objectives.

Complementary User Entity Control Considerations

Faraday's controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at Faraday and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation, and maintained at user entities as necessary to meet the trust services criteria stated in the description of Faraday's system. The table below identifies the criteria the complementary user entity controls relate to. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls	Most Relevant Criteria
Confidential information sent to Faraday is transmitted via an encrypted method.	CC6.7
Information sent to Faraday is accurate.	CC2.1
Contracts with Faraday are signed by an authorized client representative.	CC2.3
Access to transmit confidential information is limited to authorized client personnel.	CC6.5
Access to the Faraday AI System is limited to authorized individuals.	CC6.1
User passwords for the Faraday AI System are required to be complex.	CC6.1

Complementary User Entity Control Considerations (Continued)

Complementary User Entity Controls	Most Relevant Criteria
Faraday is notified of software-related issues and enhancement requests in a timely manner.	CC8.1
Security incidents are reported in a timely manner.	CC7.5

Complementary Subservice Organization Controls

Faraday's controls related to the Faraday AI System cover only a portion of overall internal control for each user entity of Faraday. It is not feasible for the trust services criteria related to Faraday AI System to be achieved solely by Faraday. Therefore, each user entity's internal control must be evaluated in conjunction with Faraday's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Complementary Subservice Organization Controls	Most Relevant Criteria
Security incidents related to security of the Faraday AI System are communicated to Faraday.	CC7.2
Physical security of the third-party data center where Faraday AI System servers are hosted is maintained.	CC6.4
System recovery controls over the third-party data center where Faraday AI System servers are hosted are maintained.	CC7.5
Environmental controls over the third-party data center where Faraday AI System servers are hosted are maintained.	CC5.2
System availability and related security policies and procedures are documented.	CC5.2
Employees are provided with ongoing security training.	CC5.2
Assessments identifying risks and threats that could impair the ability to meet user entity commitments are conducted.	CC3.1
Disaster recovery procedures are properly designed and implemented.	CC7.5
Disaster recovery procedures are regularly reviewed, updated, and tested.	CC7.5
Electronic media that contain and store confidential information are destroyed when no longer in use.	CC6.5

Section 4
Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results

Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results

Objectives of the Examination

This report is intended to provide user entities of Faraday's Faraday AI System with information about Faraday's controls pertaining to its Faraday AI System and also to provide user entities with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls in place at user entities, is intended to assist user entities in understanding the controls in place at Faraday for the services being outsourced.

In addition, Wipfli LLP's ("Wipfli") testing of controls was restricted to the categories and related controls listed in this section of the report and was not extended to all controls described in Section 3 or to controls that may be in effect at user entities. It is each interested party's responsibility to evaluate this information in relation to the controls in place at each user entity, and if certain complementary user entity controls are not in place at a user entity, Faraday's controls may not compensate for such weaknesses.

The categories and description of controls are the responsibility of Faraday's management.

Description of Testing Procedures Performed

As a part of Wipfli's examination of Faraday's controls, Wipfli performed a variety of tests, each of which provided the basis for understanding the framework for controls, and determined whether the controls were actually in place and operated effectively in accordance with Faraday's description of controls throughout the period November 1, 2020 to October 31, 2021.

Wipfli's tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified criteria were achieved throughout the period November 1, 2020 to October 31, 2021. Wipfli's tests of the operational effectiveness of the controls were designed to cover a representative number of samples throughout the period November 1, 2020 to October 31, 2021, for each of the controls listed in this section, which were designed to achieve the criteria for the specified category.

In selecting particular tests of operational effectiveness, Wipfli considered:

- The nature of the items being tested.
- The types of available evidential matter.
- The assessed level of control risk.
- The expected efficiency and effectiveness of the test.

Trust Services Categories, Criteria, and Related Controls and Independent Service Auditor's Tests of Controls and Results

Description of Testing Procedures Performed (Continued)

The procedures performed to test operating effectiveness are listed next to each of Faraday's respective control descriptions. Test procedures performed in connection with determining the operating effectiveness of the controls include the following:

Test Procedure	Description of Test Procedure
Corroborative Inquiry	Made inquiries of appropriate organizational personnel to obtain information or corroborating evidence regarding the control descriptions, processes, and procedures. **NOTE:** Because inquiries were performed for all controls, this test may not be listed individually for every control activity included in the control testing tables.
Observation	Witnessed the utilization of controls by organization personnel. This included, but was not limited to, viewing the functionality of system applications and automated controls, scheduling routines, and witnessing the processing of transactions.
Inspection	Read documents and reports that contain an indication of performance of the control. This included, but was not limited to, reading documents and reports to determine whether authorization was evidenced and transaction information was properly recorded and controlled and examining reconciliations and evidence of review to determine whether outstanding items were properly monitored, controlled, and resolved.
Reperformance	Independently performed the relevant control. This included, but was not limited to, comparing reconciliations with proper source documents, assessing the reasonableness of reconciling items, and recalculating mathematical solutions.

Results of Testing Performed

Test results are scored as "No exceptions noted," or the exception is noted.

The following tables describe the tests of operating effectiveness that were performed in meeting the categories noted. The categories, along with the criteria and the control descriptions, are an integral part of management's description of their system. The control descriptions were specified by Faraday.

Definition of Security, Availability, and Confidentiality Trust Services Categories

Security - The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

Availability - The system is available for operation and use to meet the entity's commitments and system requirements.

Confidentiality - Information designated as confidential is protected to meet the entity's commitments and system requirements.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

CC1.0 Control Environment

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Job responsibilities are communicated to and acknowledged by employees during orientation or when a job responsibility changes. Employees' roles and responsibilities are reevaluated and acknowledged annually.	Inspected the signed job descriptions for a sample of current employees to determine whether they were acknowledged.	No exceptions noted.
		An Employee Handbook that documents the Company ethical values and commitments is in place.	Inspected the Employee Handbook to determine whether it documented the Company's ethical values and commitments.	No exceptions noted.
		Background checks are performed for employees at the time of hire.	Inspected the background checks for a sample of new employees to determine whether they were completed at the time of hire.	No exceptions noted.
		An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of current employees to determine whether they were completed annually.	No exceptions noted.

CC1.0 Control Environment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	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 Board of Directors meets quarterly to discuss Company objectives and to provide oversight to management.	Inspected the Board of Directors' meeting minutes for a sample of quarters to determine whether Company objectives were discussed and oversight was provided to management.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The Board of Directors meets quarterly to discuss Company objectives and to provide oversight to management.	Inspected the Board of Directors' meeting minutes for a sample of quarters to determine whether Company objectives were discussed and oversight was provided to management.	No exceptions noted.

CC1.0 Control Environment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Job responsibilities are communicated to and acknowledged by employees during orientation or when a job responsibility changes. Employees' roles and responsibilities are reevaluated and acknowledged during the annual review process.	Inspected the signed job descriptions for a sample of current employees to determine whether they were acknowledged.	No exceptions noted.
		The organizational chart is updated as changes are made to reporting lines and authority.	Inspected the organizational chart to determine whether it was updated and reporting lines and authority were documented.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives	Faraday follows a standard recruiting process when hiring new employees.	Inspected the new hire procedure to determine whether a standard recruiting process was in place.	No exceptions noted
		Faraday uses a documented onboarding checklist when performing new hire implementation tasks.	Inspected the onboarding checklist for a sample of new employees to determine whether it was completed when performing new hire implementation tasks.	No exceptions noted.
		Security awareness training is performed for employees semiannually and for new employees at the time of hire. A security awareness training tracking log is maintained internally.	Inspected the security awareness training tracking log for a sample of current employees to determine whether security awareness training was completed semiannually.	No exceptions noted.

CC1.0 Control Environment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the security awareness training tracking log for a sample of new employees to determine whether security awareness training was completed at the time of hire.	No exceptions noted.
		Job responsibilities are communicated to and acknowledged by employees during orientation or when a job responsibility changes. Employees' roles and responsibilities are reevaluated and acknowledged during the annual review process.	Inspected the signed job descriptions for a sample of current employees to determine whether they were acknowledged.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Job responsibilities are communicated to and acknowledged by employees during orientation or when a job responsibility changes. Employees' roles and responsibilities are reevaluated and acknowledged annually.	Inspected the signed job descriptions for a sample of current employees to determine whether they were acknowledged.	No exceptions noted.

CC1.0 Control Environment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of employees to determine whether they were completed annually.	No exceptions noted.
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	No exceptions noted.
		Security awareness training is performed for new employees at the time of hire and for all employees semiannually. A security awareness training tracking log is maintained internally.	Inspected the security awareness training tracking log for a sample of current employees to determine whether security awareness training was completed semiannually.	No exceptions noted.
			Inspected the security awareness training tracking log for a sample of new employees to determine whether security awareness training was completed at the time of hire.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

CC2.0 Communication and Information

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		A documented risk assessment is updated on an ongoing basis and annually. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.

CC2.0 Communication and Information (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		A Data Retention Policy is in place. Data retention requirements are based on client contract requirements.	Inspected the Data Retention Policy to determine whether it was in place and identified retention requirements based on client contract requirements.	No exceptions noted.
		User access levels are reviewed quarterly during the Risk Committee meetings.	Inspected user access level reviews for a sample of quarters to determine whether they were performed.	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.	An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of current employees to determine whether they were completed annually.	No exceptions noted.
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	No exceptions noted.
		Security awareness training is performed for new employees at the time of hire and for all employees semiannually. A security awareness training tracking log is maintained internally.	Inspected the security awareness training tracking log for a sample of current employees to determine whether security awareness training was completed semiannually.	No exceptions noted.

CC2.0 Communication and Information (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the security awareness training tracking log for a sample of new employees to determine whether security awareness training was completed at the time of hire.	No exceptions noted.
		An Information Security Policy that documents Company responsibilities to safeguard client information is in place.	Inspected the Information Security Policy to determine whether it documented Company responsibilities to safeguard client information.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Contracts are in place for Faraday clients.	Inspected contracts for a sample of Faraday clients to determine whether contracts were in place.	No exceptions noted.
		Client responsibilities for reporting incidents, failures, and complaints are defined in the Terms of Service.	Inspected a sample client contract to determine whether client responsibilities and the Terms of Service were included.	No exceptions noted.
		Faraday has service level agreements with critical vendors.	Inspected service level agreements (SLA) for a sample of critical vendors to determine whether they were in place.	No exceptions noted.
		Faraday has Nondisclosure agreements, Business Associate Agreements (BAAs), or Security Addendums with critical vendors.	Inspected a Nondisclosure agreement, BAA, or Security Addendum for a sample of critical vendors to determine whether they were in place.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

CC3.0 Risk Assessment

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A documented risk assessment is updated on an ongoing basis. The risk assessment identifies potential threats that would impair system security, confidentiality and availability commitments and requirements, assesses risk to fraudulent actions, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.

CC3.0 Risk Assessment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A documented risk assessment is updated on an ongoing basis. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.

CC3.0 Risk Assessment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A documented risk assessment is updated on an ongoing basis. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.

CC3.0 Risk Assessment (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A documented risk assessment is updated on an ongoing basis. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.
		The Board of Directors meets quarterly to discuss Company objectives and to provide oversight to management.	Inspected the Board of Directors' meeting minutes for a sample of quarters to determine whether Company objectives were discussed and oversight was provided to management.	No exceptions noted.

CC4.0 Monitoring Activities

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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 Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.

CC4.0 Monitoring Activities (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		A documented risk assessment is updated on an ongoing basis and annually. The risk assessment identifies potential threats that would impair system security, confidentiality and availability commitments and requirements, assesses risk to fraudulent actions, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality and availability commitments and requirements, risk to fraudulent actions, analyzed the significance of those risks, and determined mitigation strategies.	No exceptions noted.
		User Access Levels are reviewed quarterly during the risk committee meetings.	Inspected user access level reviews for a sample of quarters to determine whether they were performed.	No exceptions noted.
		External vulnerability scans are performed on the network weekly.	Inspected external vulnerability scans for a sample of weeks to determine whether they were performed.	No exceptions noted.
		External penetration tests are performed on Faraday's application annually.	Inspected external penetration testing logs to determine whether they were performed regularly.	No exceptions noted.

CC4.0 Monitoring Activities (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC4.2	The entity evaluates internal control deficiencies and communicates them in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors as appropriate.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		User access levels are reviewed quarterly during the Risk Committee meetings.	Inspected user access level reviews for a sample of quarters to determine whether they were performed.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.

CC5.0 Control Activities

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Faraday has a documented Business Continuity Plan in place. Faraday has a 72-hour recovery time objective.	Inspected the Business Continuity Plan to determine whether it was in place and documented the 72-hour recovery time objective.	No exceptions noted.
		An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of employees to determine whether they were completed annually.	No exceptions noted.
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Faraday has a documented Business Continuity Plan in place. Faraday has a 72-hour recovery time objective.	Inspected the Business Continuity Plan to determine whether it was in place and documented the 72-hour recovery time objective.	No exceptions noted.

CC5.0 Control Activities (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		New device hardening procedures are documented.	Inspected the hardening procedures to determine whether they were documented.	No exceptions noted.
		Faraday has a documented network diagram made available to employees.	Inspected the network diagram to determine whether it was documented and made available to employees.	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.	An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of current employees to determine whether they were completed annually.	No exceptions noted.
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	No exceptions noted.
		Security awareness training is performed for new employees at the time of hire and for all employees semiannually. A security awareness training tracking log is maintained internally.	Inspected the security awareness training tracking log for a sample of current employees to determine whether security awareness training was completed semiannually.	No exceptions noted.

CC5.0 Control Activities (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
			Inspected the security awareness training tracking log for a sample of new employees to determine whether security awareness training was completed at the time of hire.	No exceptions noted.
		An Information Security Policy that documents Company responsibilities to safeguard client information is in place.	Inspected the Information Security Policy to determine whether it documented Company responsibilities to safeguard client information.	No exceptions noted.

CC6.0 Logical and Physical Access Controls

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		User access permissions are assigned based on job roles.	Inspected the users and access levels and compared them with the list of current employees to determine whether user access permissions were assigned based on job roles.	No exceptions noted.
		Two-factor authentication is required for Faraday's application systems. Use of a password manager is required.	Inspected the two-factor authentication and password manager screenshots to determine whether two-factor authentication and a password manager were required for Faraday's application systems.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Device firewalls are enabled on workstations.	Inspected the firewall settings for a sample of workstations to determine whether device firewalls were enabled on workstations.	No exceptions noted.
		An encrypted file transfer connection is in place for transmitting client data. Secure channels are defined, and insecure channels are not permitted.	Inspected the SFTP setup to determine whether encrypted file transfer connections were in place for transmitting client data, secure channels were defined, and insecure channels were not permitted.	No exceptions noted.
		Storage devices, databases, laptops and workstations, and infrastructure devices are encrypted at rest.	Inspected the SFTP setup to determine whether storage devices, databases, laptops and workstations, and infrastructure devices were encrypted at rest.	No exceptions noted.
		Administrative privileges to Faraday's application are limited to authorized employees.	Inspected the users and access levels and compared them with the list of current employees to determine whether administrative privileges to Faraday's application were limited to authorized employees.	No exceptions noted.
		Administrative activity is logged and monitored in logging applications.	Inspected a sample of administrative activity alerts to determine whether administrative activity was logged and monitored in logging applications.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Security groups are enabled on cloud-based environments.	Inspected the server security group to determine whether security groups were enabled on cloud-based environments.	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.	User access permissions are assigned based on job roles.	Inspected the users and access levels and compared them with the list of current employees to determine whether user access permission's were assigned based on job roles.	No exceptions noted.
		Faraday's application systems access provisioning procedures are in place to help ensure user access requests are submitted and approved by authorized employees.	Inspected the onboarding checklist for a sample of new hires to determine whether access provisioning procedures were in place to help ensure user access requests were submitted and approved by authorized employees.	No exceptions noted.
			Inspected the access provisioning procedures to determine whether access provisioning procedures were in place to help ensure user access requests were submitted and approved by authorized employees.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Faraday's application systems access termination procedures are in place to help ensure employee terminations are communicated to appropriate employees and user accounts are disabled and deleted upon notice of termination.	Inspected the termination checklist for a sample of terminated employees to determine whether termination procedures were in place to help ensure employee terminations were communicated to appropriate employees and user accounts were disabled and deleted upon notice of termination.	No exceptions noted.
			Inspected the termination procedures to determine whether access termination procedures were in place to help ensure employee terminations were communicated to appropriate employees and user accounts were disabled and deleted upon notice of termination.	No exceptions noted.
		Faraday has a documented Access Control Policy that describes expectations of user access, provisioning of user access, termination and modification of user access, and review of users' access.	Inspected the Access Control Policy to determine whether Faraday had a documented Access Control Policy that described expectations of user access, provisioning of user access, termination and modification of user access, and review of users' access.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	User access levels are reviewed quarterly during the Risk Committee meetings.	Inspected user access level reviews for a sample of quarters to determine whether they were performed.	No exceptions noted.
		User access permissions are assigned based on job roles.	Inspected the users and access levels and compared them with the list of current employees to determine whether user access permissions were assigned based on job roles.	No exceptions noted.
		Faraday's application systems access provisioning procedures are in place to help ensure user access requests are submitted and approved by authorized employees.	Inspected a sample onboarding checklist for a sample of new hires to determine whether access provisioning procedures were in place to help ensure user access requests were submitted and approved by authorized employees.	No exceptions noted.
			Inspected the access provisioning procedures to determine whether access provisioning procedures were in place to help ensure user access requests were submitted and approved by authorized employees.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Faraday's application systems access termination procedures are in place to help ensure employee terminations are communicated to appropriate employees and user accounts are disabled and deleted upon notice of termination.	Inspected the termination checklist for a sample of terminated employees to determine whether termination procedures were in place to help ensure employee terminations were communicated to appropriate employees and user accounts were disabled and deleted upon notice of termination.	No exceptions noted.
			Inspected the termination procedures to determine whether access termination procedures were in place to help ensure employee terminations were communicated to appropriate employees and user accounts were disabled and deleted upon notice of termination.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A- Faraday is not responsible for restricting physical access to facilities hosting the Faraday AI System.		

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	Documented data retention and disposal procedures are in place to guide the secure disposal of the Company's and clients data.	Inspected the Data Sanitization Policy to determine whether documented data retention and disposal procedures were in place to guide the secure disposal of the Company's and clients' data.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		User access permissions are assigned based on job roles.	Inspected the users and access levels and compared them with the list of current employees to determine whether user access permissions were assigned based on job roles.	No exceptions noted.
		Two-factor authentication is required for Faraday's application systems. Use of a password manager is required.	Inspected the two-factor authentication and password manager screenshots to determine whether two-factor authentication and a password manager were required for Faraday's application systems.	No exceptions noted.
		Device firewalls are enabled on workstations.	Inspected the firewall settings for a sample of workstations to determine whether device firewalls were enabled on workstations.	No exceptions noted.
		An encrypted file transfer connection is in place for transmitting client data. Secure channels are defined, and insecure channels are not permitted.	Inspected the SFTP setup to determine whether encrypted file transfer connections were in place for transmitting client data, secure channels were defined, and insecure channels were not permitted.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Storage devices, databases, laptops and workstations, and infrastructure devices are encrypted at rest.	Inspected the SFTP setup to determine whether storage devices, databases, laptops and workstations, and infrastructure devices were encrypted at rest.	No exceptions noted.
		Security groups are enabled on cloud-based environments.	Inspected the server security group to determine whether security groups were enabled on cloud-based environments.	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.	An encrypted file transfer connection is in place for transmitting client data. Secure channels are defined, and insecure channels are not permitted.	Inspected the SFTP setup to determine whether encrypted file transfer connections were in place for transmitting client data, secure channels were defined, and insecure channels were not permitted.	No exceptions noted.
		Storage devices, databases, laptops and workstations, and infrastructure devices are encrypted at rest.	Inspected the SFTP setup to determine whether storage devices, databases, laptops and workstations, and infrastructure devices were encrypted at rest.	No exceptions noted.

CC6.0 Logical and Physical Access Controls (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		Antivirus and malware software is installed on workstations.	Inspected antivirus and malware software scans for a sample of workstations to determine whether antivirus and malware software was installed.	No exceptions noted.
		Antivirus software and malware software are configured to check for updates regularly, and scans are performed semiannually.	Inspected the workstation antivirus configurations to determine whether antivirus software and malware software were configured to check for updates regularly and scans were performed semiannually.	No exceptions noted.
		Server instances are rebuilt monthly to help prevent the existence of unauthorized or malicious software.	Inspected the server instances screenshot for a sample of servers to determine whether they were rebuilt monthly.	No exceptions noted.

Criteria, Related Controls, and Independent Auditor's Tests of Controls and Results

CC7.0 System Operations

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	External vulnerability scans are performed on the network weekly.	Inspected external vulnerability scans for a sample of weeks to determine whether they were performed.	No exceptions noted.
		External penetration tests are performed on Faraday's application annually.	Inspected external penetration testing logs to determine whether external penetration tests were performed regularly.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.

CC7.0 System Operations (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		Antivirus and malware software is installed on workstations.	Inspected antivirus and malware software scans for a sample of workstations to determine whether antivirus and malware software was installed.	No exceptions noted.
		Antivirus software and malware software are configured to check for updates regularly, and scans are performed semiannually.	Inspected the workstation antivirus configurations to determine whether antivirus software and malware software were configured to check for updates regularly and scans were performed semiannually.	No exceptions noted.

CC7.0 System Operations (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		Client responsibilities for reporting incidents, failures, and complaints are defined in the Terms of Service.	Inspected a sample client contract to determine whether client responsibilities and the Terms of Service were included.	No exceptions noted.
		A documented Security Incident Response Plan is in place.	Inspected the Security Incident Response Plan to determine whether it was in place.	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.	Client responsibilities for reporting incidents, failures, and complaints are defined in the Terms of Service.	Inspected a sample client contract to determine whether client responsibilities and the Terms of Service were included.	No exceptions noted.
		A documented Security Incident Response Plan is in place.	Inspected the Security Incident Response Plan to determine whether it was in place.	No exceptions noted.

CC7.0 System Operations (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A documented Security Incident Response Policy is in place.	Inspected the Security Incident Response Plan to determine whether it was in place.	No exceptions noted.
		Faraday has a documented Business Continuity Plan in place. Faraday has a 72-hour recovery time objective.	Inspected the Business Continuity Plan to determine whether it was in place and documented the 72-hour recovery time objective.	No exceptions noted.
		Application servers are reconstructed monthly to help determine whether data restores are operating effectively.	Inspected application server reconstruction reports for a sample of months to determine whether server provisioning software was functioning.	No exceptions noted.

CC8.0 Change Management

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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 Software Development Life Cycle (SDLC) Policy includes gathering requirements, design, testing, acceptance, and deployment of software.	Inspected the SDLC Policy to determine whether the policy included gathering requirements, design, testing, acceptance, and deployment of software.	No exceptions noted.
		Progress is tracked in industry-standard issue tracking software. Source code is version controlled.	Inspected the software development procedures to determine whether progress was tracked in industry-standard issue tracking software and source code was version controlled.	No exceptions noted.
			Inspected the software change tickets for a sample of software changes to determine whether changes were tracked in industry-standard issue tracking software and source code was version controlled.	No exceptions noted.
		Separate environments are used for development, testing, and production.	Inspected the software development procedures to determine whether separate environments were used for development, testing, and production.	No exceptions noted.
			Inspected the version control tracking software screenshot to determine whether separate environments were used for development, testing, and production.	No exceptions noted.

CC8.0 Change Management (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		New device hardening procedures are documented.	Inspected the hardening procedures to determine whether they were documented.	No exceptions noted.
		Servers are patched monthly as part of the monthly server reconstruction procedure.	Inspected the server patch status screenshot for a sample of Faraday servers to determine whether patches were installed monthly as part of the monthly server reconstruction procedure.	No exceptions noted.
		Workstations are updated for patches semiannually.	Inspected the workstation patch status screenshot for a sample of Faraday servers to determine whether patches were installed semiannually.	No exceptions noted.

CC9.0 Risk Mitigation

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A documented risk assessment is updated on an ongoing basis and annually. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		The Risk Committee meets quarterly and includes a discussion related to Company policies, operations, events, changes, and related risk requirements as part of the agenda as needed.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine whether Company policies, operations, events, changes, and related risk requirements were discussed.	No exceptions noted.
		SOC Reports and Complimentary User Entity Controls are reviewed for critical vendors as part of the overall Vendor Due Diligence Program.	Inspected SOC report reviews for a sample of critical vendors to determine whether they were reviewed.	No exceptions noted.

CC9.0 Risk Mitigation (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Faraday personnel request, obtain, and read their third-party vendors' SOC Reports to ensure they include control activities covering the following areas: • Computer operations • Change management • Logical access • Physical security • Protection against environmental factors • Power outages • Backup redundancy	Inspected a sample SOC report review to determine whether it included a review of control activities covering the following areas: • Computer operations • Change management • Logical access • Physical security • Protection against environmental factors • Power outages • Backup redundancy	No exceptions noted.
		Faraday has a documented Business Continuity Plan in place. Faraday has a 72-hour recovery time objective.	Inspected the Business Continuity Plan to determine whether it was in place and documented the 72-hour recovery time objective.	No exceptions noted.

CC9.0 Risk Mitigation (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A documented risk assessment is updated on an ongoing basis and annually. The risk assessment identifies potential threats that would impair system security, confidentiality, and availability commitments and requirements; assesses risk of fraudulent actions; analyzes the significance of risks associated with the identified threats; and determines mitigation strategies for those risks.	Inspected the Information Risk Assessment to determine whether it identified potential threats that would impair system security, confidentiality, and availability commitments and requirements; assessed risk of fraudulent actions; analyzed the significance of those risks; and determined mitigation strategies.	No exceptions noted.
		Faraday has SLAs with critical vendors.	Inspected SLAs for a sample of critical vendors to determine whether they were in place.	No exceptions noted.
		Faraday has Nondisclosure agreements, BAAs, or Security Addendums with critical vendors.	Inspected a Nondisclosure agreement, BAA, or Security Addendum for a sample of critical vendors to determine whether they were in place.	No exceptions noted.

CC9.0 Risk Mitigation (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		SOC Reports and Complimentary User Entity Controls are reviewed for critical vendors as part of the overall Vendor Due Diligence Program.	Inspected SOC report reviews for a sample of critical vendors to determine whether they were reviewed.	No exceptions noted.
		Faraday personnel request, obtain, and read their third-party vendors' SOC Exams to ensure they include control activities covering the following areas: • Computer operations • Change management • Logical access • Physical security • Protection against environmental factors • Power outages • Backup redundancy	Inspected a sample SOC report review to determine whether it included a review of control activities covering the following areas: • Computer operations • Change management • Logical access • Physical security • Protection against environmental factors • Power outages • Backup redundancy	No exceptions noted.

Additional Information Related to Availability

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
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	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		Application servers are reconstructed monthly to help determine whether server provisioning software is functioning.	Inspected application server reconstruction reports for a sample of months to determine whether server provisioning software was functioning.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	SOC Reports and Complimentary User Entity Controls are reviewed for critical vendors as part of the overall Vendor Due Diligence Program.	Inspected SOC report reviews for a sample of critical vendors to determine whether they were reviewed.	No exceptions noted.

Additional Information Related to Availability (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring software configurations to determine whether it was configured to identify and evaluate system performance, security threats, resource utilization needs, and unusual system activity.	No exceptions noted.
			Inspected a sample of alerts to determine whether monitoring software identified and notified of system performance, security threats, resource utilization, and unusual system activity.	No exceptions noted.
		Application servers are reconstructed monthly to help determine whether server provisioning software is functioning.	Inspected application server reconstruction reports for a sample of months to determine whether server provisioning software was functioning.	No exceptions noted.
		Faraday has a documented network diagram made available to employees.	Inspected the network diagram to determine whether it was documented and made available to employees.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Database server point-in-time recovery tests are performed semiannually to help ensure data can be restored in the event of a disaster.	Inspected semiannual database server point-in-time recovery test documentation to determine whether databases were tested for restoration purposes.	No exceptions noted.

Additional Information Related to Availability (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
		Application servers are reconstructed monthly to help determine if server provisioning software is functioning.	Inspected application server reconstruction reports for a sample of months to determine whether server provisioning software was functioning.	No exceptions noted.
		Faraday has a documented Business Continuity Plan in place. Faraday has a 72-hour recovery time objective.	Inspected the Business Continuity Plan to determine whether it was in place and documented the 72-hour recovery time objective.	No exceptions noted.

Additional Information Related to Confidentiality

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A Data Retention Policy is in place. Data retention requirements are based on client contract requirements.	Inspected the Data Retention Policy to determine whether it was in place and identified retention requirements based on client contract requirements.	No exceptions noted.
		An acknowledgement of the Employee Handbook and the Employee and Service Provider Information Security Agreement is completed annually. The Employee and Service Provider Information Security Agreement includes employee responsibility in regard to confidentiality and protection of information and data.	Inspected the Employee Handbook acknowledgment and the Employee and Service Provider Information Security Agreement for a sample of current employees to determine whether they were completed annually.	No exceptions noted.
			Inspected the Employee and Service Provider Information Security Agreement to determine whether it included employee responsibilities regarding confidentiality and protection of information and data.	No exceptions noted.
		A Vendor Management Policy is in place and includes confidentiality requirements.	Inspected the Vendor Management Policy to determine whether it was in place included confidentiality requirements.	No exceptions noted.

Additional Information Related to Confidentiality (Continued)

Criteria Number	Criteria Description	Control Description	Description of Testing	Results of Testing
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	Documented data retention and disposal procedures are in place to guide the secure disposal of the Company's and clients' data.	Inspected the Data Sanitization Policy to determine whether documented data retention and disposal procedures were in place to guide the secure disposal of the Company's and client' data.	No exceptions noted.