Pequity

TYPE 2

SOC 2® Report

Controls Relevant to Security, Availability, and Confidentiality

For the Period September 1, 2023 to August 31, 2024

Prepared in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA)

SOC 2 Automated by Drata

mjd ADVISORS

AICPA SOC aicpa.org/soc4so SOC for Service Organizations ™

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor’s Report

To the Management of Pequity, Inc.
Trout Run, Pennsylvania

Scope

We have examined Pequity, Inc.’s (the Company) accompanying description in Section 3 titled “Management’s Description of the Pequity Platform” throughout the period September 1, 2023 to August 31, 2024 (description) based on the criteria for a description of a service organization’s system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Service Organization’s Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to ensure the Company’s service commitments and system requirements were achieved. The Company has provided the accompanying assertion in Section 2 titled “Assertion of Pequity, Inc. Management” (assertion) about the description and suitability of the design and operating effectiveness of controls. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted following attestation standards established by the AICPA. Those standards require 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 whether the controls stated were suitably designed and operating effectively to provide reasonable assurance the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

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

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

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

Inherent Limitations

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in the accompanying "Information Provided by Service Auditor" in Section 4.

Opinion

In our opinion, in all material respects:

a) The description presents the Pequity Platform that was designed and implemented throughout the period September 1, 2023 to August 31, 2024, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period and if the subservice organizations applied the complementary controls assumed in the design of the Company's controls throughout the period.

c) The controls stated in the description operated effectively throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Company's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Company, user entities of the Pequity Platform during some or all of the period September 1, 2023 to August 31, 2024, business partners of the Company subject to risks arising from interactions with the Pequity Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

MJD Advisors

Waukee, Iowa
September 27, 2024

Section 2

Management’s Assertion

Assertion of Pequity, Inc. Management

Management of Pequity, Inc. has prepared the accompanying description titled “Management’s Description of the Pequity Platform” throughout the period September 1, 2023 to August 31, 2024, based on the criteria for a description of a service organization’s system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*). The description is intended to provide report users with information about the Pequity Platform that may be useful when assessing the risks arising from interactions with the Pequity Platform, particularly information about system controls the Company 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 set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

a) The description presents the Pequity Platform that was designed and implemented throughout the period September 1, 2023 to August 31, 2024, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that the Company’s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period September 1, 2023 to August 31, 2024, and if the subservice organizations applied the complementary controls assumed in the design of the Company’s controls throughout the period September 1, 2023 to August 31, 2024.

c) The controls stated in the description operated effectively throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Company’s controls operated effectively throughout that period.

Management of Pequity, Inc.
September 27, 2024

Section 3

System Description

System Description

Management’s Description of the Pequity Platform
For the Period September 1, 2023 to August 31, 2024

Types of Services Provided

The Pequity Platform (Pequity or the Platform) is designed to simplify and streamline compensation programs and help organizations attract and retain world-class talent. Through an interactive web application and integrations with human resources and applicant tracking systems, Pequity provides a single source of truth for the information driving compensation and hiring decisions and allows users to benchmark internally and externally to improve pay decision accuracy and efficiency. The key objectives of the Platform are to facilitate the following for its users:

- Internal collaboration amongst key stakeholders to streamline the candidate compensation approval process.
- Analysis of market data to benchmark current and prospective employees' pay and evaluate hiring trends.
- Pay philosophy development through compensation ranges based on a candidate's experience and geographic location.
- Oversee the organization’s applicant tracking system and understand the hiring pipeline within the context of workforce metrics.
- Support companies as they go through the process of managing their compensation cycles.

Pequity, Inc. is responsible for the development and maintenance of the Platform, which is hosted on cloud computing infrastructure and made available to customers in a web application format. The Platform integrates with customer human resources information systems to pull employee compensation data and embeds the information with their applicant tracking system to enable the core functionalities described above.

Principal Service Commitments and System Requirements

Management’s Description of the Pequity Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization’s service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to customers through software-as-a-service agreements and information shared on the Company's website. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- The Company protects the security and integrity of all client data that is collected, accessed, stored, or received by the Company in connection with the Platform.
- The Company maintains a written comprehensive security program with administrative, technical, and physical safeguards to protect client data.
- The Company implements procedures to prohibit the unauthorized use, disclosure, duplication, misuse or removal of confidential information.
- The Company performs automatic backups of all customer and system data weekly.
- The Company provides access to customer data on the principle of least privilege.
- Encryption technologies are used to protect customer data at rest and in transit.
- Multi-factor authentication is mandatory for access to sensitive resources and implemented for other systems when possible.
- Firewalls and intrusion detection systems are used to protect systems from intrusion and limit the scope of any successful attack.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.

Components of the System

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

The components of the Platform can be classified into the following five categories:

Infrastructure: The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications, desktop, or laptop applications.

People: The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

Data: The types of data used by the system, such as transaction streams, files, databases, tables, and other outputs used or processed by the system.

Procedures: The automated and manual procedures related to the services provided, including procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

The Company's infrastructure is managed through a cloud hosting model with the primary services supported by Digital Ocean (DO) and Amazon Web Services (AWS) (the Cloud Providers). The Company leverages the Cloud Providers to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met.

The specific services utilized to support the Platform's cloud infrastructure include the following:

Cloud Hosting Services	
Service	**Description**
DO Droplets	On-demand Linux virtual machines
DO Managed PostgreSQL Database	Managed PostgreSQL database service
DO Spaces	Object storage
DO Managed Redis	Managed key-value database service
DO Virtual Private Cloud	Provides a logically isolated virtual network for the production environment to control traffic
DO Managed MySQL Database	Managed MySQL database service
AWS S3	Object storage
AWS ECS	Managed container service
Amazon ElastiCache for Redis	Redis-compatible in-memory data store
AWS Fargate	Serverless compute engine for containers
AWS WAF	Web application firewall
Amazon RDS	Managed relational database service
AWS Parameter Store	Configuration data and secrets management
AWS KMS	Cryptographic key management
AWS IAM	Identity and access management for AWS resources
Amazon GuardDuty	Threat detection service
Amazon ECR	Managed container registry
Amazon CloudWatch	Infrastructure resource and application monitoring
AWS CloudTrail	Infrastructure audit logging
Application Load Balancer	Managed load-balancing service
AWS Virtual Private Cloud	Provides a logically isolated virtual network that uses network security groups to control traffic

Software

Software consists of the programs and software that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Software Summary	
Application	**Purpose**
Drata	Compliance management platform
GitHub	Source code repository
GitHub Dependabot	Dependency scanning
GitHub Actions	CI/CD
Google Workspace	File storage, email, document collaboration, identity provider
Terraform	Infrastructure as code
Jira	Project management and issue tracking
Slack	Communication hub
Clickup	Project management and issue tracking
QA Wolf, Cucumber	Automated testing software
SonarQube	Code quality and security testing
Heap, Pendo	User analytics
ClamAV	Antivirus
MergeQueue	Merge workflow automation
Sentry	Application monitoring and error tracking
Rippling	Human resource information system and access management
Twingate	Infrastructure access management
Rootkit Hunter	Antivirus
Ubuntu Unattended Upgrades	Infrastructure scanning and patching
Cloudflare	Managed web application firewall
Fail2Ban	Intrusion detection software
Certn	Background checks
Figma	Collaborative design
Datadog	Monitoring and alerting
Datadog Security	Real-time threat detection and continuous configuration audits

Critical Tools and Resources

The Information Security Program and scope of the system description apply to all infrastructure and software identified in the previous sections. Control activities and procedures are applied to internal systems using a risk-based approach that primarily considers the sensitivity of information stored or processed by the system and its role in maintaining the security, availability, and confidentiality of the Company's information. The systems deemed by management to be vital to meeting its service commitments and system requirements are defined as "Critical Tools and Resources" throughout this description. They include the following:

- Digital Ocean
- AWS
- Twingate
- GitHub
- Google Workspace
- Terraform

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	**Function**
Board of Directors	Responsible for governance, oversight of management, and major decision-making, representing the interests of shareholders and includes members independent of management
CEO	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities
Security Officer	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Security Team	Cross-functional team responsible for oversight, implementation, and continual improvement of the Information Security Program
Engineering	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security
Leadership	Responsible for operations, legal, and engineering leadership that support strategic decision-making and ongoing operations of the Company
Growth	Interfaces routinely with prospective clients and existing clients to build pipeline, increase sales, and maintain relationships to limit customer churn

The Company leverages a remote workforce for the Platform’s management, operation, and security with individuals worldwide. Certain individuals within the Company’s core team may be hired legally as independent contractors but are subject to identical controls as individuals hired as “employees” within the context of this system description; thus, both classes are defined as “personnel” throughout the report.

The Company may also work with other individuals hired for a specific project or a defined period. The Company performs a risk assessment for these individuals, as defined in the vendor management process. Controls are implemented based on risk factors, such as level of access and responsibility for sensitive information. These individuals are described as “contractors” within the remaining scope of this description.

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management’s statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions. The Company has adopted the following defined set of information security standards and policies (described as the Information Security Program throughout the report):

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity Plan
- Code of Conduct
- Data Classification Policy
- Data Retention Policy
- Data Protection Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Response Plan
- Information Security Policy
- Password Policy
- Physical Security Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Lifecycle Policy
- System Access Control Policy
- Vendor Management Policy
- Vulnerability Management Policy

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners.

The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary

Type	Description	Storage and Processing
Account data	Personally Identifiable Information and other administrative data from personnel, customers, and other third parties	Digital Ocean, AWS, and other 3rd party technology providers
Secrets	Access credentials, tokens, certificates, API keys, and other secrets	AWS Parameter Store, AWS KMS
Log information	Information relevant to and explicitly necessary for services, including metadata	Amazon CloudWatch, AWS CloudTrail, Datadog, Sentry
Analytics data	Product usage and tracking data are sent to analytics services to analyze usage patterns and inform product decisions	Heap, Pendo

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements for the period September 1, 2023 to August 31, 2024.

Applicable Trust Services Criteria and Related Controls

The trust services criteria are classified into five categories: security, availability, processing integrity, confidentiality, and privacy. Depending on which category or categories are included within the scope of the description, the applicable trust services criteria consist of criteria common to all five of the trust services criteria (common criteria) and additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories. The common criteria constitute the complete set of criteria for the security category.

The trust services category or categories in scope for this report are as follows:

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.

Availability: Information and systems are available for operation and use to meet the entity's objectives.

Confidentiality: Information designated as confidential is protected to meet the entity's objectives.

The common criteria are organized as follows:

Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Communication and Information: Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

Risk Assessment: The entity's identification and analysis of relevant risks to achieving its objectives, forming a basis for determining how the risks can be managed.

Monitoring Activities: The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of controls, and acts to address deficiencies identified.

Control Activities: The policies and procedures that help make sure that management's directives are carried out.

Logical and Physical Access Controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.

System Operations: The criteria relevant to how the entity manages the operation of systems and detects and mitigates processing deviations, including logical and physical security deviations.

Change Management: The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

Risk Mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Environment

The Company’s control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. A control environment is the foundation on which an effective system of internal control is built and operated in an organization that strives to achieve its strategic objectives, provide reliable reporting to internal and external stakeholders, operate its business efficiently and effectively, comply with all applicable laws and regulations, and safeguard its assets.

Integrity and Ethical Values

Integrity and ethical behavior are the products of the Company’s ethical and behavioral standards, communicated, monitored, and enforced in its business activities. The Company's standards of conduct outline its commitments to integrity and ethical values and the details are made available to all personnel. These commitments include management’s actions to remove or reduce incentives, pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts.

Oversight Responsibility

The Company has a formal Board of Directors that includes individuals independent of management. The Board of Directors is responsible for governance and oversight, including defining the expectations for integrity and ethics. The CEO reports to the Board of Directors each quarter to discuss high-level objectives and resource allocation and allows the independent board members to provide guidance, direction, and accountability for management.

Organizational Structure, Authority, and Responsibility

The Company’s organizational structure provides the framework within which its activities for achieving objectives are planned, executed, and monitored. A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel. Management established the operating structure based on its size and the nature of its control environment and designed reporting lines to establish key areas of authority and the proper flow of information. Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program. Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.

Commitment to Competence

Management demonstrates its commitment to competence through established policies and practices that attract, develop, and retain sufficient and competent individuals to support the achievement of objectives. The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year. The primary objective of the security training program is to educate personnel on their responsibility to protect the confidentiality, availability, and integrity of the Company’s information.

Management has established formal and informal procedures that consider the background and technical competency of potential and existing personnel and vendors when determining whether to hire or retain the individual. Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.

Accountability

The Company expects individuals to be held accountable for their internal control responsibilities in pursuing objectives. Management establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct and considering the achievement of both short-term and long-term objectives. Individual performance is evaluated through periodic one-on-one sessions and regular feedback provided informally.

External Individuals

The Company's commitment to integrity and ethical values extends to its use of contractors and vendors. Management considers the use of service providers, who may impact security, confidentiality, and privacy in its processes to establish conduct standards, evaluate adherence to those standards, and promptly address deviations. Information security requirements for mitigating the risks associated with a supplier's access to the Company's assets are formalized with the supplier and documented.

Service providers, such as contractors, who may impact the security of the production environment or have access to customer data, are required to read and accept a non-disclosure agreement. As a general practice, the Company leverages the services of vendors generally accepted in the industry and typically shares their commitments towards security, confidentiality, and privacy available to the public, which is reviewed by personnel to ensure consistency with the Company's policies.

Communication and Information

A critical objective for the Company is ensuring relevant and quality information is obtained or generated to support the functioning of internal control. The Company has established processes to identify information requirements and ensure appropriate internal and external sources of information are properly captured to support the functioning of other internal control components. Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.

Internal Communication

The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel. Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually. Management also reinforces the Information Security Program in meetings, internal communication, and during annual security training and awareness programs.

Management has established specific communication channels to ensure personnel have the necessary information to understand and carry out their internal control responsibilities. Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held frequently to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. The Company considers the timing, audience, and nature of the information when selecting the appropriate communication medium, allowing management to communicate changes to control objectives in a timely manner.

The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls. Formal procedures are established and documented in the Company's plans for incident response that describes how to report system failures, incidents, concerns, and other complaints to personnel.

External Communication

The Company has prioritized maintaining open communication channels with external parties that allow input from customers, business partners, external auditors, and others to provide management with relevant information. The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations. Agreements are established with critical vendors and business partners that clearly define terms, conditions, and responsibilities. Security objectives and commitments are made available to customers through software-as-a-service agreements and information shared on the Company's website.

The Company makes information available about the design and operation of the Platform and its boundaries to users through user guides and other resources shared through the public website. Customers and other external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.

Product updates are shared with customers so the Company can continue to innovate and maintain the security of the Platform. Multiple marketing channels are available to share new features, and the Company selects the appropriate method, frequency, and messaging based on the specific feature being shared. Product updates that impact user functionality or security are communicated to users directly via email or other methods, as deemed appropriate. Significant changes, such as those that require action by the user to maintain functionality or impact security requirements, are communicated to users directly and in advance of the implementation.

Risk Assessment

The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks. The first step of the risk assessment process is to identify assets within the scope of the Information Security Program. The objectives identified by management are specified in the risk management program to enable the identification and assessment of risk related to the objectives.

The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to assets and service commitments are identified, and the risks are formally assessed. The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information.

Risk management discussions include a consideration of how changes in the environment impact risk, such as revisions to the Company's business model, personnel turnover, and the implementation of new systems and technology, which may create new risks that could significantly impact the Company's ability to meet its objectives. The Security Team meets on a quarterly basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.

Monitoring Activities

The Company selects, develops, and performs ongoing and, if necessary, separate evaluations to ascertain whether the components of internal control are present and functioning. Management considers the rate of change in business and business processes when selecting and developing separate ongoing evaluations and utilizes the current state of the internal controls to establish a baseline. The following describes the primary methods currently utilized by management:

> **Penetration Testing:** The Company engages third parties to conduct penetration tests of the production environment at least annually. The penetration tests are performed by a certified penetration tester to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Management reviews the results, and high-priority findings are tracked to resolution.
>
> **Dependency Scanning:** GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Updates identified are scored for compatibility, categorized by risk, and pull requests are automatically created for review in GitHub. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.
>
> **Bug Bounty Program:** The Company has implemented a bug bounty program that is communicated to security researchers in the HackerOne community. HackerOne provides vulnerability coordination and connects the Company with crowd-sourced, independent, security monitoring. Vulnerabilities are submitted to management, evaluated for severity, and mitigated according to risk.

Static Code Analysis: The Company utilizes Sonarqube to identify vulnerabilities or coding flaws that pose cybersecurity threats. Scanning offers coverage of the OWASP Top 10 and provides issue descriptions and code highlights to explain potential code risks. Alerts are provided to management and remediated according to risk assessment.

Intrusion Detection: The Company utilizes Fail2Ban to scan log files and identify suspicious activity on DigitalOcean droplets. Firewall rulesets are automatically updated to reject new connections from IP addresses with greater than five unsuccessful authentication attempts. The company uses Clamav and Rootkit Hunter to detect eventual trojans and rootkits.

Threat Detection: Amazon GuardDuty has been enabled to continuously monitor for malicious behavior to protect AWS accounts. The service combines machine learning, anomaly detection, network monitoring, and malicious file discovery, using both AWS and industry-leading third-party sources to help protect workloads and data on AWS. Alerts are configured to notify management of unusual activity and promptly reviewed for potential impact to the Platform.

Monitoring of Cloud Environment: The Company evaluates risks related to the Cloud Providers and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary. Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel. Production systems are configured to monitor, log, and self-repair or alert on suspicious changes to critical system files and unauthorized intrusions and access attempts.

Access Logs: The Company maintains user access logs for privileged access and for access to user data, which are periodically reviewed by the Security Officer. Logical access to audit logs is restricted to authorized personnel, and system administrators are not permitted to erase or deactivate logs of their own activities.

The results of ongoing and separate evaluations are provided to the appropriate individuals to assess results. The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.

Control Activities

Control activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to achieve objectives are carried out. They may be preventative or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

Compliance Management Platform

Management leverages a compliance management platform (Drata) to support the design, implementation, operation, monitoring, and documentation of its control activities. The platform captures data via APIs across multiple technology providers, including identity providers, infrastructure providers, version control systems, ticketing systems, and human resource information systems, to provide a central dashboard for compliance activities.

Drata is also utilized to support the following:

- Continuous automated monitoring of certain security controls
- Compliance checks on personnel workstations
- Inventory management
- Communication and documentation of review, approval, and acknowledgment of information security policies
- Real-time visibility to manage the Information Security Program

Use of a compliance management platform does not relieve management of its responsibilities for designing, implementing, and operating the Information Security Program. Management is also responsible for evaluating the accuracy and completeness of the information produced, maintained, and aggregated by Drata, which is performed through an annual risk assessment and necessary due diligence procedures, such as obtaining and reviewing the platform's most recent SOC 2 Type 2 report; which includes the trust services criteria related to processing integrity.

Information Security Program Development and Maintenance

As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. The risk assessment process includes the selection and development of control activities over technology infrastructure, designed and implemented to help ensure the completeness, accuracy, and availability of technology processing. Specifically, management selects and develops control activities designed and implemented to restrict technology access rights and achieve management's objectives over the acquisition, development, and maintenance of technology and infrastructure.

The Information Security Program is reviewed by management annually and formally approved. The Company's policies and procedures are designed to govern an individual's day-to-day activities and establish expectations and relevant procedures specifying actions. Management assigns competent personnel with sufficient authority the responsibility to promptly perform control activities and duties with diligence and continuing focus.

Confidential Information

The Company has implemented control activities to protect confidential information throughout its lifecycle, including collection, processing, and disposal as described in formal policies within the Information Security Program. The Company's data management policies have been established to define the Company's data classification practices in accordance with legal requirements, sensitivity, and business criticality to ensure information is classified, protected, retained, and securely disposed of in accordance with its importance. Data owners are responsible for identifying additional requirements for specific data or exceptions to standard handling requirements. The Company has implemented the following classes of data:

Data Classification

Class	Description	Examples
Confidential	Highly sensitive data requiring the highest level of protection. Access is restricted to specific individuals based on a principle of least privilege, and explicit authorization by the Security Officer is required for access	Data protected by state or federal privacy regulations (e.g. PHI & PII), confidentiality agreements, and other commitments to third parties
Internal	Company proprietary information requires thorough protection with access restricted to individuals based on business requirements and requires approval for distribution outside the company	Internal policies, meeting minutes, contracts, messages, emails, internal reports
Public	Documents intended for public consumption, which can be freely distributed outside the Company	Marketing materials, product descriptions, release notes, external facing policies

Data is classified as Confidential unless it has been explicitly classified as an alternative category and the information is isolated to specific data stores. The Company's data management policies include requirements for data handling, retention, and disposal procedures for the Company's accounts and devices. Customer information is retained in accordance with laws and regulations which are outlined in the Company's internal and external policies and communication. Data is deleted upon the request of the customer and expired account data will be removed after 14 days.

Logical and Physical Access Controls

The Company has established policies and procedures that define the access control requirements for requesting and provisioning user access to the system. Duties and access to sensitive resources are established based on the principle of least privilege. Logical access to systems is restricted through access control software and rule sets and is controlled by limited administrative users. Individuals require a unique username and are identified and authenticated before accessing information assets. Access to Critical Tools and Resources requires multi-factor authentication.

The Company has established a formal onboarding and termination process. Appropriate management approval is obtained before granting access to Critical Tools and Resources. The Company's compliance management platform performs automated checks and triggers alerts if users access certain resources without appropriate approval and completion of the onboarding process. The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels. Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

Privileged access to Critical Tools and Resources is highly restricted. Users with multiple access levels (e.g., administrators) are given separate accounts for normal system use and administrative functions. The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection. Access to migrate changes to production is restricted to authorized individuals with a business need.

Full-disk encryption is implemented for all personnel workstations and laptops. Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.

Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company. Information and data assets are subject to the Company's policies and procedures for data protection, classification, and retention, which define parameters for the ownership, classification, security, storage, and retention of data. Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.

The Pequity Platform is built upon a multi-tenancy architecture; thus every subdomain (and every Platform client) is proxied by Cloudflare. The Platform uses a public-key certificate to protect the domains, and Cloudflare is configured to require traffic utilizing TLS 1.2 or greater. Encryption is used to protect customer data at rest. Processes are in place to protect encryption keys during generation, storage, use, and destruction.

Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The Company uses firewalls and configures them to protect against threats from sources outside the system's boundaries. The Company uses Cloudflare as a DNS manager and network-based firewall to protect from further security threats and ensure availability and capacity.

System Operations

The Company has established baseline configuration standards and uses tools to detect and restore configuration deviations from the standards. Infrastructure is monitored for noncompliance with the configuration standards, which could threaten the achievement of the Company's objectives. Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis. Identified security deficiencies are tracked and prioritized through internal tools according to their severity.

Applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once the patches have been reviewed and their criticality level is determined, service teams determine the patch implementation strategy.

Formal procedures are defined for security event detection and management, including the provision of resources. The Company uses a system that collects and stores logs in a central location. The system can be queried in an ad hoc fashion by authorized users. Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.

The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents. Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence. Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals. Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned. The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.

Processing capacity and usage are monitored on an automatic, real-time basis to appropriately manage capacity demand. Services generally provide for automated provisioning of additional resources to scale vertically and horizontally as needed without action by the Company's personnel.

The Platform is hosted in multiple regions, designed to fail independently, thus allowing the Platform to remain available when any single region fails. Load balancers are used to automatically distribute incoming application traffic across multiple instances and regions.

Business and system recovery plans are documented, which provide the roles and responsibilities and detailed procedures for the recovery of systems. The Company has documented plans for business continuity and disaster recovery that are reviewed, tested, and updated on an annual basis. Backups are configured to run automatically, and production data is replicated in different regions. The integrity and completeness of backup information are tested annually.

Change Management

The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems. The change management processes and procedures have been established to plan, schedule, apply, distribute, and track changes to the production environment to minimize risk and client impact.

The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Software developers are expected to adhere to the Company's coding standards throughout the development cycle, including standards for quality, commenting, and security. Releases are tested throughout the development process and validated prior to the deployment. Testing is performed in an isolated environment that is separate from production workloads.

Code changes include a formal code review process. Only experienced and knowledgeable engineers with experience in code review techniques and secure coding practices can approve a code change. Overrides of edit checks, approvals, and changes to confirmed transactions are appropriately authorized, documented, and reviewed. Access to migrate changes to production is restricted to authorized individuals with a business need. Deployment systems are configured to automatically alert the Company's personnel in Slack for any change to the code repository and any release to the production environment.

Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the Company's commitments and system requirements. Upon the identification of a deficiency, processes are in place for authorizing, designing, testing, approving, and implementing changes necessary in the event a change needs to be implemented in an urgent timeframe.

Risk Mitigation

The Company implements risk mitigation strategies to prioritize, evaluate, and implement the appropriate risk-reducing controls recommended by the risk management process. Management has identified potential business disruptions as a critical risk to meeting its objectives and has established plans for business continuity, disaster recovery, and incident response to respond to, mitigate, and recover from security events that could disrupt business operations. These plans are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents. Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.

As part of its risk mitigation strategies, management assesses and manages risks associated with vendors and business partners. Periodically, generally annually, but performed relative to risk and changes in the environment, management assesses the risks that vendors and business partners represent to the achievement of the Company's objectives. As a general practice, the Company utilizes software and infrastructure resources and applications that are industry leaders and generally accepted amongst the security community.

The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided, and other factors, and a review of the vendor's security and privacy requirements. Based on the risk assessment, management obtains due diligence and compliance information, such as SOC 2 Type 2 reports, requested and reviewed during the vendor acceptance and re-review process. The Company has written agreements in place with vendors and business partners that include confidentiality and privacy commitments consistent with the commitments and requirements of the Company.

User Entity Controls and Responsibilities

The Company's services are designed utilizing a shared responsibility model where maintaining the security of a customer's information is dependent upon the customer implementing controls that are outside the Company's control. If these controls are necessary to meet the Company's service commitments and system requirements, they are known as complementary user entity controls (CUECs) as defined by DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*. Other controls that are necessary or recommended for the customer to maintain the security, availability, and confidentiality of its information are defined as user entity responsibilities.

Complementary User Entity Controls

The Company has restricted its service commitments to matters for which it is responsible and that can be reasonably achieved by itself, and the Platform's system requirements are derived from those commitments. Therefore, CUECs are not required or significant to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

The Company communicates the expectations or requirements of its users through legal agreements and instructional material, such as user manuals, which are necessary to allow the customer to benefit from the use of the Platform. User entity responsibilities are generally either explicitly required or communicated as a recommended best practice, and the controls presented below should not be regarded as a comprehensive list of controls that user entities should implement.

User entity responsibilities that should be implemented to allow the customer to benefit from the use of the Platform include the following:

- Ensuring the confidentiality of user accounts and passwords
- Notifying the Company promptly when changes are made to technical, billing, or administrative contact information
- Developing internal disaster recovery and business continuity plans that address the inability to access or utilize the Company's services
- Notifying the Company and providing accurate information regarding new, terminated, and changes necessary to user accounts
- Informing the Company of any regulatory issues that may affect the services provided
- Understanding and complying with contractual obligations to the Company
- Immediately notifying the Company of any actual or suspected information security breaches involving the Platform, including compromised user accounts
- Granting access only to authorized and trained personnel
- Deploying physical security and environmental controls for all devices and access points

Subservice Organization Controls

When controls at a vendor are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved, based on the applicable trust services criteria, the vendor is considered a subservice organization. Complementary subservice organization controls (CSOCs) are controls that the Company's management assumed, in the design of the system, would be implemented by subservice organizations and are necessary, in combination with controls at the Company, to provide reasonable assurance that the Company's service commitments and system requirements were achieved. Management has identified the below subservice organizations and has elected to use the carve-out method for the purposes of this report:

Complementary Subservice Organizations	
Subservice Organization	**Description**
Digital Ocean and AWS	Cloud hosting services

The Company has implemented procedures for the oversight and monitoring of the services provided by the subservice organizations, which are outlined in the vendor management policies and procedures. Personnel are highly trained to manage the cloud infrastructure and regularly review technical resources made available through technical training and industry forums to understand key concepts and implement controls necessary to meet the Company's responsibilities described in the shared responsibility model for each specific service utilized. Management also reviews available compliance reports and monitors the subservice organizations through regular communication and interaction with the environment.

The following are the applicable trust services criteria and controls that are necessary to be in place at the subservice organizations to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Subservice Organization Controls	
Criteria	**Control**
Logical and Physical Access CC6 Series	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.

Complementary Subservice Organization Controls	
Criteria	**Control**
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.
Change Management CC8 Series	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.
Availability A Series	Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure. Environmental protections, data backup processes, and recovery mechanisms have been implemented and appropriately tested to adequately address availability requirements.

Trust Services Criteria Relevance

All security, availability, and confidentiality trust services criteria as set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* were relevant to the Platform as presented in this report.

Significant Changes to the Platform

During the period September 1, 2023 to August 31, 2024, the Company began migrating the Platform's cloud-hosted infrastructure from DigitalOcean to AWS utilizing a similar selection of managed service offerings. Customer production accounts have been transferred from DigitalOcean to AWS in batches as part of a phased migration plan which is anticipated to be completed in September 2024. The transition has not impacted the Company's ability to meet its service commitments and system requirements.

Use of Report

The description does not omit or distort information relevant to the Platform while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to their own particular needs.

Section 4

Information Provided by Service Auditor

Information Provided by Service Auditor

Engagement Objectives and Scope

A SOC 2 report is intended to provide users of the Pequity Platform with the information necessary to help assess and address the risks associated with the services provided by the Platform. The report is intended for use by those with sufficient knowledge and understanding of the Platform, its services, and the system used to provide those services, among other matters. Without such knowledge, users are likely to misunderstand the contents of the SOC 2 report. Thus the Independent Service Auditor's Report of MJD Advisors, LLC (MJD) provided in Section 1 is restricted to specified parties with the requisite knowledge.

MJD's responsibility in this report is to perform a SOC 2 examination in accordance with AT-C Section 105, *Concepts Common to All Attestation Engagements*, and AT-C Section 205, *Examination Engagements*. According to those standards, the examination is predicated on the concept that management is responsible for the design, implementation, and operating effectiveness of its controls to provide reasonable assurance the organization's service commitments and system requirements were achieved. Management is also responsible for preparing the System Description in Section 3 and Management's Assertion in Section 2 of this report, including the completeness, accuracy, and method of presentation. MJD's responsibility is to design and perform procedures to obtain sufficient appropriate evidence and express an opinion on the presentation of the description and the design and operating effectiveness of controls.

Management of Pequity, Inc. is responsible for determining the point in time (SOC 2 Type 1) or period of time (SOC 2 Type 2) to be covered by the description of the Platform, its assertion, and, consequently, the service auditor's examination. The frequency and period covered by a SOC 2 report is a business decision of management, determined by the needs of its users, and management determined that a SOC 2 Type 2 report was appropriate in the circumstances. MJD's responsibility is to express an opinion on the description and the suitability of the design and operating effectiveness of controls, further described in Section 1.

Compliance Management Platform

As described in the Control Activities section of the System Description, management leverages a compliance management platform (Drata) to support the design, implementation, operation, monitoring, and documentation of its control activities. Drata is also used by management to enhance the efficiency of the examination by collecting and organizing the Company's documentation in a central repository that is supported by integrated data connections. Information generated by Drata and made available to MJD as audit evidence is considered information provided by the Company. Management is expected to have evaluated the accuracy and completeness of the information produced and maintained.

The responsibility of MJD to obtain sufficient appropriate evidence to support the Independent Service Auditor's Report is unchanged by management's use of Drata. MJD performed certain procedures to determine whether Drata functioned as intended and whether the information generated by Drata was reliable for MJD's purposes. Specifically, MJD reviewed Drata's most recently available SOC 2 Type 2 Report, which included the trust services criteria related to processing integrity.

Control Matrix for the Pequity Platform

The control matrix that follows is to provide report users with the specific controls management has identified to meet the applicable trust services criteria. MJD's tests of the operating effectiveness of those controls included such tests considered necessary in the circumstances to evaluate whether those controls were sufficient to provide reasonable, but not absolute, assurance the Company's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security, availability, and confidentiality throughout the period September 1, 2023 to August 31, 2024.

Tests of controls included inquiry of appropriate management, supervisory and staff personnel, observation of the Company's activities and operations, and inspection of documents and records. In selecting particular tests of the operating effectiveness of the controls, we considered multiple factors, such as (*a*) the characteristics of the population of the controls to be tested, including the nature of the controls; (*b*) whether the population is made up of homogenous items; (*c*) the frequency of the controls' application; and (*d*) the expected deviation rate. Where appropriate, we utilized a sample-based testing strategy in accordance with the AICPA Audit Guide, *Audit Sampling*, developed by the AICPA *Audit Sampling* Guide Task Force. As inquiries were performed for substantially all the Company's controls, this test was not listed individually for every control in the control matrix below.

For tests of controls requiring the use of information produced by the entity (IPE), MJD performed one or more of the following procedures to address the completeness, accuracy, and data integrity of the data or reports provided:

- Inspected the source of the data or report
- Inspected the query, script, or parameters used to generate the data or report
- Observed the generation of the data or report
- Agreed data between the report and the source

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access listings), MJD evaluated management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or report.

Control Matrix for the Pequity Platform

Control Environment

CC1.1: The entity demonstrates a commitment to integrity and ethical values.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's standards of conduct outline its commitments to integrity and ethical values and the details are made available to all personnel.	Inspected the Company's standards of conduct to determine they outlined a commitment to integrity and ethical values. Observed evidence the Company makes the standards of conduct available to all personnel.	No deviations noted.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.	Inspected the most recent signed acknowledgment of the Information Security Program and standards of conduct for a selection of current personnel to ascertain it was completed within the required time frame. Inspected signed acknowledgments of the Information Security Program and standards of conduct for a selection of new personnel to ascertain it was completed upon hire.	No deviations noted.
Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.	Inspected the Information Security Program to ascertain the requirements for background verification checks to be performed on personnel before onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks. Inspected background verification checks or other evidence for a selection of new personnel to ascertain background screening procedures were performed based on the perceived risk of the position.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for a selection of critical vendors to ascertain management reviewed the terms of service, privacy policy, and other information provided by the vendor, as needed, to determine the security, confidentiality, and privacy commitments were consistent with the requirements established by the Company.	No deviations noted.

Control Environment

CC1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Description	Tests Performed by MJD	Results
The Company has a formal Board of Directors that includes individuals independent of management.	Inspected the biographies of the members of the Board of Directors to ascertain the governance body included members independent of management.	No deviations noted.
The CEO reports to the Board of Directors each quarter to discuss high-level objectives and resource allocation and allows the independent board members to provide guidance, direction, and accountability for management.	Obtained the Board of Directors' meeting minutes prepared throughout the scope period to ascertain the meeting was held at least quarterly.	No deviations noted.

CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Description	Tests Performed by MJD	Results
A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel.	Inspected the organizational chart to ascertain it defined areas of authority, responsibility, and reporting lines.	No deviations noted.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.	Inspected the Information Security Program to ascertain it formally assigned the responsibility for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	No deviations noted.
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.	Inspected the Company’s online job postings and the job description template to ascertain the requirements and responsibilities for new positions are documented and communicated for new positions.	No deviations noted.

Control Environment

CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Description	Tests Performed by MJD	Results
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.	Inspected the most recent signed acknowledgment of the Information Security Program and standards of conduct for a selection of current personnel to ascertain it was completed within the required time frame. Inspected signed acknowledgments of the Information Security Program and standards of conduct for a selection of new personnel to ascertain it was completed upon hire.	No deviations noted.
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.	Inspected the Company's online job postings and the job description template to ascertain the requirements and responsibilities for new positions are documented and communicated for new positions.	No deviations noted.
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.	Inspected evidence of the most recently completed security training program for a selection of current personnel to ascertain it had been performed within the required time frame. Inspected evidence of the completion of the security training program for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.	Inspected the Information Security Program to ascertain the requirements for background verification checks to be performed on personnel before onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks. Inspected background verification checks or other evidence for a selection of new personnel to ascertain background screening procedures were performed based on the perceived risk of the position.	No deviations noted.

Control Environment

CC1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's standards of conduct outline its commitments to integrity and ethical values and the details are made available to all personnel.	Inspected the Company's standards of conduct to determine they outlined a commitment to integrity and ethical values. Observed evidence the Company makes the standards of conduct available to all personnel.	No deviations noted.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.	Inspected the most recent signed acknowledgment of the Information Security Program and standards of conduct for a selection of current personnel to ascertain it was completed within the required time frame. Inspected signed acknowledgments of the Information Security Program and standards of conduct for a selection of new personnel to ascertain it was completed upon hire.	No deviations noted.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.	Inspected the Information Security Program to ascertain it formally assigned the responsibility for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	No deviations noted.

Communication and Information

CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Description	Tests Performed by MJD	Results
Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.	Inspected the architecture diagram to determine it documented system boundaries and observed evidence it was made available to personnel.	No deviations noted.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel.	No deviations noted.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.

Communication and Information

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.	Inspected evidence of the most recently completed security training program for a selection of current personnel to ascertain it had been performed within the required time frame. Inspected evidence of the completion of the security training program for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.	Inspected the architecture diagram to determine it documented system boundaries and observed evidence it was made available to personnel.	No deviations noted.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel.	No deviations noted.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.	Inspected the most recent signed acknowledgment of the Information Security Program and standards of conduct for a selection of current personnel to ascertain it was completed within the required time frame. Inspected signed acknowledgments of the Information Security Program and standards of conduct for a selection of new personnel to ascertain it was completed upon hire.	No deviations noted.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.	Inspected the Information Security Program to ascertain it formally assigned the design, development, implementation, operation, maintenance, and monitoring of system controls.	No deviations noted.

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
Formal procedures are established and documented in the Company’s plans for incident response that describes how to report system failures, incidents, concerns, and other complaints to personnel.	Inspected the procedures and plans for incident response to ascertain the policies and procedures provide guidance for reporting security failures, incidents, concerns, and other complaints to appropriate personnel.	No deviations noted.

Communication and Information

CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
Security objectives and commitments are made available to customers through software-as-a-service agreements and information shared on the Company's website.	Inspected the software-as-a-service agreement template and the Platform's public website to ascertain the Company communicates its security objectives and commitments to customers.	No deviations noted.
The Company makes information available about the design and operation of the Platform and its boundaries to users through user guides and other resources shared through the public website.	Inspected the Platform's website to ascertain information is made available to users to understand the design and operation of the Platform and its boundaries.	No deviations noted.
Customers and other external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the Company's website to ascertain it provided contact information for reporting system failures, incidents, concerns, and other complaints to appropriate personnel.	No deviations noted.
Product updates that impact user functionality or security are communicated to users directly via email or other methods, as deemed appropriate.	Observed example communications sent to users to announce product changes to ascertain the Company has channels in place to communicate changes to the Platform.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for a selection of critical vendors to ascertain management reviewed the terms of service, privacy policy, and other information provided by the vendor, as needed, to determine the security, confidentiality, and privacy commitments were consistent with the requirements established by the Company.	No deviations noted.

Risk Assessment

CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The objectives identified by management are specified in the risk management program to enable the identification and assessment of risk related to the objectives.	Inspected the annual risk assessment and discussed the process with management to determine that the Company specified its objectives to enable the identification and assessment of risks related to objectives.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.

Risk Assessment

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.

Control Description	Tests Performed by MJD	Results
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Security Team meets on a quarterly basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.	Inspected evidence of Security Team meetings throughout the scope period to ascertain the group met on a quarterly basis.	No deviations noted.

CC3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information.	Inspected the risk management program to ascertain the Company's fraud risk assessment is to include consideration of incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from the IT and access to information.	No deviations noted.

Risk Assessment

CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Description	Tests Performed by MJD	Results
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Security Team meets on a quarterly basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.	Inspected evidence of Security Team meetings throughout the scope period to ascertain the group met on a quarterly basis.	No deviations noted.

Monitoring Activities

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.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company’s vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
The Company evaluates risks related to the Cloud Providers and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary.	Inspected evidence of management's risk assessment and annual review of the SOC 2 reports for the Cloud Providers.	No deviations noted.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for the Company's log aggregation tool to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.

Monitoring Activities

CC4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company’s vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
The Company evaluates risks related to the Cloud Providers and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary.	Inspected evidence of management's risk assessment and annual review of the SOC 2 reports for the Cloud Providers.	No deviations noted.
The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.	Observed the use of any dashboards for the Company's ticketing system to ascertain deficiencies are aggregated centrally, assigned to the individual responsible for corrective action, and provided visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.

Control Activities

CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Description	Tests Performed by MJD	Results
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Inspected the risk management program to ascertain the risk management process is designed to be integrated with the selection or development of control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Information Security Program is reviewed by management annually and formally approved.	Inspected evidence the Information Security Program was reviewed and formally approved by management within the previous 12 months.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.

Control Activities

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Description	Tests Performed by MJD	Results
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Inspected the risk management program to ascertain the risk management process is designed to be integrated with the selection or development of control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Information Security Program is reviewed by management annually and formally approved.	Inspected evidence the Information Security Program was reviewed and formally approved by management within the previous 12 months.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.	Inspected the configuration of the compliance management platform and observed management's systems for monitoring access levels to ascertain access to Critical Tools and Resources is continually monitored.	No deviations noted.

Control Activities

CC5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel.	No deviations noted.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.	Inspected the Information Security Program to ascertain it formally assigned the design, development, implementation, operation, maintenance, and monitoring of system controls.	No deviations noted.
Security objectives and commitments are made available to customers through software-as-a-service agreements and information shared on the Company's website.	Inspected the software-as-a-service agreement template and the Platform's public website to ascertain the Company communicates its security objectives and commitments to customers.	No deviations noted.
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Information Security Program is reviewed by management annually and formally approved.	Inspected evidence the Information Security Program was reviewed and formally approved by management within the previous 12 months.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.

Logical and Physical Access Controls

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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Access to Critical Tools and Resources requires multi-factor authentication.	Inspected the Information Security Program to ascertain the requirement to use multi-factor authentication to access the Company's systems. Inspected the configuration of Critical Tools and Resources to ascertain multi-factor authentication was enforced for all users.	No deviations noted.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.	Inspected the configuration of the compliance management platform and observed management's systems for monitoring access levels to ascertain access to Critical Tools and Resources is continually monitored.	No deviations noted.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection.	Inspected the Information Security Program to ascertain the requirement for remote access to be strictly controlled with encryption. Inspected the configuration for the production environment to ascertain access is restricted to encrypted channels.	No deviations noted.
Access to migrate changes to production is restricted to authorized individuals with a business need.	Inspected the user access listings and reviewed individuals with the ability to deploy changes to the production environment with management to ascertain privileged access was restricted to appropriate individuals.	No deviations noted.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Description	Tests Performed by MJD	Results
Encryption is used to protect customer data at rest.	Inspected the configuration of systems storing customer data at rest or other evidence as deemed appropriate to ascertain the data was encrypted.	No deviations noted.
Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis.	Inspected the configuration of the Ubuntu unattended upgrades package to ascertain the package runs daily to scan infrastructure resources for vulnerabilities and install automatic security upgrades.	No deviations noted.

Logical and Physical Access Controls

CC6.2: Before 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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.	Inspected the Company's policies and procedures for access management to ascertain the requirements for obtaining management approval prior to granting access to systems. Inspected evidence appropriate authorization had been established prior to granting access to Critical Tools and Resources for a selection of new personnel.	No deviations noted.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.	Inspected the configuration of the compliance management platform and observed management's systems for monitoring access levels to ascertain access to Critical Tools and Resources is continually monitored.	No deviations noted.
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day. Inspected evidence to demonstrate access removal for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within one business day.	No deviations noted.

Logical and Physical Access Controls

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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Individuals require a unique username and are identified and authenticated before accessing information assets.	Inspected the user listings for Critical Tools and Resources to ascertain each user was assigned a unique username.	No deviations noted.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.	Inspected the Company's policies and procedures for access management to ascertain the requirements for obtaining management approval prior to granting access to systems. Inspected evidence appropriate authorization had been established prior to granting access to Critical Tools and Resources for a selection of new personnel.	No deviations noted.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.	Inspected the configuration of the compliance management platform and observed management's systems for monitoring access levels to ascertain access to Critical Tools and Resources is continually monitored.	No deviations noted.
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day. Inspected evidence to demonstrate access removal for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within one business day.	No deviations noted.

Logical and Physical Access Controls

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.

The physical security of the Company’s primary resources has been outsourced through a cloud-hosting model, and these controls are carved out for the purposes of this report.

See Subservice Organizations described within Section 3.

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.

Control Description	Tests Performed by MJD	Results
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day. Inspected evidence to demonstrate access removal for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within one business day.	No deviations noted.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.
Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.	Inspected the Company's Information Security Program to ascertain formal procedures have been established to guide the secure retention and disposal of Company data.	No deviations noted.

Logical and Physical Access Controls

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Description	Tests Performed by MJD	Results
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for the Company's log aggregation tool to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.
Access to Critical Tools and Resources requires multi-factor authentication.	Inspected the Information Security Program to ascertain the requirement to use multi-factor authentication to access the Company's systems. Inspected the configuration of Critical Tools and Resources to ascertain multi-factor authentication was enforced for all users.	No deviations noted.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection.	Inspected the Information Security Program to ascertain the requirement for remote access to be strictly controlled with encryption. Inspected the configuration for the production environment to ascertain access is restricted to encrypted channels.	No deviations noted.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected configurations and other sources of evidence to ascertain the Platform uses secure data protocols consistent with its service commitments and system requirements.	No deviations noted.
The Company utilizes Fail2Ban to scan log files and identify suspicious activity on DigitalOcean droplets. Firewall rulesets are automatically updated to reject new connections from IP addresses with greater than five unsuccessful authentication attempts.	Observed the DigitalOcean firewall ruleset, list of Fail2Ban jailed IP addresses, and example slack notifications to ascertain that the Company utilizes Fail2Ban to identify suspicious activity and firewall rulesets are automatically updated when security threats are detected.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Description	Tests Performed by MJD	Results
Amazon GuardDuty has been enabled to continuously monitor for malicious behavior to protect AWS accounts. Alerts are configured to notify management of unusual activity and promptly reviewed for potential impact to the Platform.	Observed the Amazon GuardDuty dashboard to ascertain continuous monitoring of the Platform's network was in place to detect security threats, including access anomalies. Observed the communication channels and example alerts to ascertain personnel are notified when security threats are detected.	No deviations noted.
Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis.	Inspected the configuration of the Ubuntu unattended upgrades package to ascertain the package runs daily to scan infrastructure resources for vulnerabilities and install automatic security upgrades.	No deviations 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.		
Control Description	**Tests Performed by MJD**	**Results**
Full-disk encryption is implemented for all personnel workstations and laptops.	Inspected monitoring results from the compliance management platform for a selection of personnel to ascertain the individuals utilized computers with full-disk encryption.	No deviations noted.
Encryption is used to protect customer data at rest.	Inspected the configuration of systems storing customer data at rest or other evidence as deemed appropriate to ascertain the data was encrypted.	No deviations noted.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected configurations and other sources of evidence to ascertain the Platform uses secure data protocols consistent with its service commitments and system requirements.	No deviations noted.
The Company uses firewalls and configures them to protect against threats from sources outside the boundaries of the system.	Inspected the configuration of the firewalls to ascertain the firewall was appropriately deployed to deny all traffic by default unless explicitly allowed.	No deviations noted.
Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis.	Inspected the configuration of the Ubuntu unattended upgrades package to ascertain the package runs daily to scan infrastructure resources for vulnerabilities and install automatic security upgrades.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for the Company's log aggregation tool to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.	Inspected evidence for a selection of personnel to ascertain they utilized computers with the most recent operating system security updates and configured with antivirus software.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Description	Tests Performed by MJD	Results
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.
Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis.	Inspected the configuration of the Ubuntu unattended upgrades package to ascertain the package runs daily to scan infrastructure resources for vulnerabilities and install automatic security upgrades.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring had been implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.
Infrastructure resources are scanned for vulnerabilities and automatic security upgrades are installed on a daily basis.	Inspected the configuration of the Ubuntu unattended upgrades package to ascertain the package runs daily to scan infrastructure resources for vulnerabilities and install automatic security upgrades.	No deviations noted.

System Operations

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.

Control Description	Tests Performed by MJD	Results
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company’s vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
The Company utilizes Fail2Ban to scan log files and identify suspicious activity on DigitalOcean droplets. Firewall rulesets are automatically updated to reject new connections from IP addresses with greater than five unsuccessful authentication attempts.	Observed the DigitalOcean firewall ruleset, list of Fail2Ban jailed IP addresses, and example slack notifications to ascertain that the Company utilizes Fail2Ban to identify suspicious activity and firewall rulesets are automatically updated when security threats are detected.	No deviations noted.
Amazon GuardDuty has been enabled to continuously monitor for malicious behavior to protect AWS accounts. Alerts are configured to notify management of unusual activity and promptly reviewed for potential impact to the Platform.	Observed the Amazon GuardDuty dashboard to ascertain continuous monitoring of the Platform’s network was in place to detect security threats, including access anomalies. Observed the communication channels and example alerts to ascertain personnel are notified when security threats are detected.	No deviations noted.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for the Company’s ticketing system to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control Description	Tests Performed by MJD	Results
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring had been implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.

System Operations

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.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company’s vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Vulnerabilities identified are regularly reviewed by management and assigned for remediation as required.	Inspected the dashboard for GitHub Dependabot to ascertain the service was enabled and reviewed the status of outstanding vulnerabilities with management to determine whether a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for the Company’s ticketing system to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.
The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents.	Inspected the Company's policies and plans for incident response to ascertain the responsibilities of management had been outlined and procedures were documented to respond to information security incidents.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received, and personnel quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue had been retained.	No deviations noted.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Description	Tests Performed by MJD	Results
Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals.	Inspected the Company's policies and plans for incident response to ascertain it provided guidelines and expectations for communication with management, users, and other key individuals to share the necessary information regarding security events.	No deviations noted.

System Operations

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.

Control Description	Tests Performed by MJD	Results
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring had been implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received, and personnel quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue had been retained.	No deviations noted.
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for creating, prioritizing, and tracking follow-ups to completion. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain personnel tracked the event and followed up to completion. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

System Operations

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.		
Control Description	**Tests Performed by MJD**	**Results**
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for the Company’s ticketing system to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.
The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents.	Inspected the Company's policies and plans for incident response to ascertain the responsibilities of management had been outlined and procedures were documented to respond to information security incidents.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received, and personnel quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue had been retained.	No deviations noted.
Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for conducting post-mortem meetings for security incidents to discuss the root causes, remediation steps, and lessons learned. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Description	Tests Performed by MJD	Results
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for creating, prioritizing, and tracking follow-ups to completion. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain personnel tracked the event and followed up to completion. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Description	Tests Performed by MJD	Results
Product updates that impact user functionality or security are communicated to users directly via email or other methods, as deemed appropriate.	Observed example communications sent to users to announce product changes to ascertain the Company has channels in place to communicate changes to the Platform.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Access to migrate changes to production is restricted to authorized individuals with a business need.	Inspected the user access listings and reviewed individuals with the ability to deploy changes to the production environment with management to ascertain privileged access was restricted to appropriate individuals.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company’s policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.
The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	Inspected configurations and observed the use of version control software to manage source code, documentation, release labeling, and other change management tasks.	No deviations noted.
Releases are tested throughout the development process and validated prior to the deployment.	Inspected the workflow requirements to ascertain the requirement for testing to be performed before deployment.	No deviations noted.
Testing is performed in an isolated environment that is separate from production workloads.	Inspected evidence that the production environment resources are isolated from development systems.	No deviations noted.

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
Control Description	**Tests Performed by MJD**	**Results**
Code changes include a formal code review process. Only experienced and knowledgeable engineers with experience in code review techniques and secure coding practices can approve a code change.	Inspected the configurations of the code repository to ascertain branch protections are in place, requiring a review before deployment.	No deviations noted.
Deployment systems are configured to automatically alert the Company's personnel in Slack for any change to the code repository and any release to the production environment.	Observed the Slack channel to ascertain the integration with the deployment systems was active, and the channel included the appropriate personnel.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
Control Description	**Tests Performed by MJD**	**Results**
The Company’s plans for business continuity, disaster recovery, and incident response are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Company's plans for business continuity, disaster recovery, and incident response to ascertain each outlined guidance for detecting, responding to, and recovering from security events and incidents. Observed evidence the Company's plans for business continuity, disaster recovery, and incident response are made available to Company personnel.	No deviations noted.
Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.	Inspected the Company's cybersecurity insurance policy to ascertain it was in place to mitigate the financial impact of business disruptions.	No deviations noted.

Risk Mitigation

CC9.2: The entity assesses and manages risks associated with vendors and business partners.		
Control Description	**Tests Performed by MJD**	**Results**
The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security, confidentiality, and privacy requirements.	Inspected the Company's policies for vendor management to ascertain procedures include maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security and privacy requirements. Obtained the inventory of third-party vendors, reviewed the categorization of vendor risks, and inspected documentation supporting management's review and risk assessment for vendors that store or process data on behalf of customers or perform other high-risk functions related to the Platform.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for a selection of critical vendors to ascertain management reviewed the terms of service, privacy policy, and other information provided by the vendor, as needed, to determine the security, confidentiality, and privacy commitments were consistent with the requirements established by the Company.	No deviations noted.

Additional Criteria for Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control Description	Tests Performed by MJD	Results
Processing capacity and usage are monitored on an automatic, real-time basis to appropriately manage capacity demand.	Inspected the dashboard for the cloud monitoring tools and alerting channels to ascertain processing and usage are subject to monitoring, and thresholds are established for alerting personnel.	No deviations noted.
Load balancers are used to automatically distribute incoming application traffic across multiple instances and regions.	Observed the cloud provider administrative console to verify a load balancer was implemented to automatically distribute incoming application traffic across multiple instances and regions.	No deviations noted.
Services generally provide for automated provisioning of additional resources to scale vertically and horizontally as needed without action by the Company's personnel.	Observed the cloud provider administrative console and architecture diagram and reviewed developer documentation provided by the cloud provider to ascertain the primary services utilized by the Company provide for the automated provisioning of resources when predefined capacity thresholds are met.	No deviations noted.

Additional Criteria for Availability

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.

Control Description	Tests Performed by MJD	Results
The Company has documented plans for business continuity and disaster recovery that are reviewed, tested, and updated on an annual basis.	Inspected the plans prepared for business continuity and disaster recovery and verified each was reviewed and approved by management in the previous 12 months. Inspected the results of the tests performed on the business continuity and disaster recovery plans to ascertain the procedure was performed in the previous 12 months.	No deviations noted.
Backups are configured to run automatically, and production data is replicated in different regions.	Inspected the configuration of the backup service to ascertain automated backups have been established consistent with the Company's recovery strategy.	No deviations noted.
The integrity and completeness of backup information are tested annually.	Inspected the results of the backup recovery test to ascertain it was completed in the previous 12 months.	No deviations noted.

Additional Criteria for Availability

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has documented plans for business continuity and disaster recovery that are reviewed, tested, and updated on an annual basis.	Inspected the plans prepared for business continuity and disaster recovery and verified each was reviewed and approved by management in the previous 12 months. Inspected the results of the tests performed on the business continuity and disaster recovery plans to ascertain the procedure was performed in the previous 12 months.	No deviations noted.
The integrity and completeness of backup information are tested annually.	Inspected the results of the backup recovery test to ascertain it was completed in the previous 12 months.	No deviations noted.

Additional Criteria for Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's data classification and management policies have been established to define the Company's data classification practices in accordance with legal requirements, sensitivity, and business criticality to ensure information is classified, protected, retained, and securely disposed of in accordance with its importance.	Inspected the Company's policies for data classification and management to ascertain the Information Security Program defines the Company's data classification practices in accordance with legal requirements, sensitivity, and business criticality.	No deviations noted.
Data is classified as Confidential unless it has been explicitly classified as an alternative category and the information is isolated to specific data stores.	Inspected the Company's policies for data classification to ascertain the requirement for all data to be treated as Confidential unless it is explicitly classified as an alternative category and isolated to specific data stores. Inspected the Company's network diagram and reviewed the flow of information with management to ascertain the processes for categorizing customer data and the systematic approach to isolate confidential information to specific data stores.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Encryption is used to protect customer data at rest.	Inspected the configuration of systems storing customer data at rest or other evidence as deemed appropriate to ascertain the data was encrypted.	No deviations noted.

Additional Criteria for Confidentiality

C1.2: The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.		
Control Description	**Tests Performed by MJD**	**Results**
The Company’s data classification and management policies have been established to define the Company’s data classification practices in accordance with legal requirements, sensitivity, and business criticality to ensure information is classified, protected, retained, and securely disposed of in accordance with its importance.	Inspected the Company’s policies for data classification and management to ascertain the Information Security Program defines the Company’s data classification practices in accordance with legal requirements, sensitivity, and business criticality.	No deviations noted.
Data is deleted upon the request of the customer, and expired account data will be removed after 14 days.	Inspected the Company’s internal and external policies for data retention to ascertain the requirement that data is required to be removed within 14 days.	No deviations noted.

End of Report