dmarcian, Inc.

DMARC Management Platform

System and Organization Controls (SOC) for Service Organizations Report for the period of April 1, 2022 to February 28, 2023

FORVIS

An Independent Service Auditor Report issued by
FORVIS, LLP

Table of Contents

FORVIS

Section I: Report of Independent Service Auditors

To: Management of dmarcian, Inc.

Scope

We have examined dmarcian, Inc.'s (the "Company") accompanying description of its DMARC Management Platform (the "System") titled *dmarcian, Inc.'s Description of its System and Controls* throughout the period April 1, 2022 to February 28, 2023, (the "description") based on the criteria for a description of a service organization's System in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (the "description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the period April 1, 2022 to February 28, 2023, 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 privacy (the "applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses Google LLC, a subservice organization, to provide third-party hosting of virtual servers and administrative 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 organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity 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 complementary user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *dmarcian, Inc.'s Assertion* (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. 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.

FORVIS

Service Auditor's Responsibilities

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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; and
- Evaluating the overall presentation of the description.

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV of this report.

FORVIS

Opinion

In our opinion, in all material respects,

A. The description presents dmarcian, Inc.'s DMARC Management Platform that was designed and implemented throughout the period April 1, 2022 to February 28, 2023, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the period April 1, 2022 to February 28, 2023, to provide reasonable assurance that dmarcian, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of dmarcian, Inc.'s controls throughout that period.

C. The controls stated in the description operated effectively throughout the period April 1, 2022 to February 28, 2023, to provide reasonable assurance that dmarcian, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of dmarcian, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period April 1, 2022 to February 28, 2023, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

FORVIS, LLP

Tysons, VA

July 11, 2023

Section II: dmarcian, Inc.'s Assertion

We have prepared the accompanying description of dmarcian, Inc.'s (the "Company") DMARC Management Platform (the "System") titled *dmarcian, Inc.'s Description of its System and Controls* throughout the period April 1, 2022 to February 28, 2023 (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (the "description criteria"). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with the Company's System, particularly information about system controls that 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 privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses Google LLC, a subservice organization, to provide third-party hosting of virtual servers and administration 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 organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related 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 complementary user entity controls assumed in the design of the Company's controls.

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

A. The description presents the System that was designed and implemented throughout the period April 1, 2022 to February 28, 2023, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the period April 1, 2022 to February 28, 2023 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 that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period.

C. The controls stated in the description operated effectively throughout the period April 1, 2022 to February 28, 2023 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

Section III: dmarcian, Inc.'s Description of its System and Controls

A. Overview of Services Provided

This report only covers the services provided by dmarcian, Inc. ("dmarcian" or the "Company") and their DMARC Management Platform.

Founded in 2012 by one of the primary authors of the Domain-based Message Authentication, Reporting, & Conformance (DMARC) specification, dmarcian is dedicated to upgrading the entire world's email by making DMARC accessible to all. dmarcian has global operations and serving six continental regions. From small governmental organizations, to Fortune 500 companies, dmarcian has an international track record for helping organizations across the globe and of all sizes successfully deploy DMARC.

dmarcian brings together thousands of senders, vendors, and operators in a common effort to build DMARC into the email ecosystem. Customers range from banks, top Internet properties, governments, marketing agencies, telecoms, and commercial enterprises of all sizes. dmarcian users enjoy access to expert support, powerful tools, human friendly articles and videos, and a growing global network of DMARC deployment partners. dmarcian has offices around the world in key locations of North America, Canada, Europe, and Asia Pacific. dmarcian prides itself on being a champion of DMARC and partners with organizations such as the Global Cyber Alliance (GCA), the Online Trust Alliance (OTA), the Certified Senders Alliance (CSA), and the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG).

dmarcian's purpose is to spread DMARC far and wide by increasing education, accessibility, advocacy, and thought leadership. dmarcian achieves this by focusing on the people doing the work and helping them make the world of email and the greater world a better place for all.

DMARC Management Platform

dmarcian's DMARC Management Platform receives, processes, and classifies DMARC data observed from users' domain namespace and makes sense of it for the user. The native Extensible Markup Language (XML) format in which DMARC data is transmitted is not intended for human consumption. The Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) standard are security mechanisms which prevent unauthorized individuals from sending emails on a user's behalf. The platform visualizes the data in powerful and meaningful ways so users can quickly identify authentication gaps (SPF/DKIM) and unauthorized use of their domains.

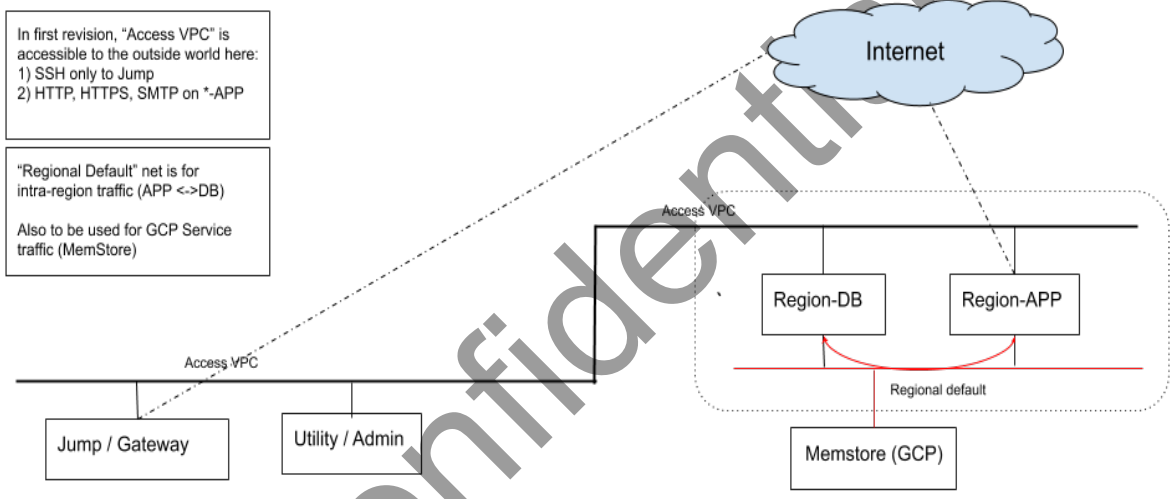
In addition to aggregating DMARC data, the platform provides domain administration teams with the necessary features to adopt DMARC with clarity and confidence. The dmarcian reporting platform sits atop as an accurate source classification engine in the industry and affords users with assurances of the true origin of a particular mail stream. The DMARC Management platform enables users with the ability to utilize the following features:

- Free Web-based tools which allow users to search email domains for SPF, DKIM, and DMARC records.
- Monitoring and Reporting of XML data relevant to SPF/DKIM/DMARC records. The platform receives, processes, and classifies mail observed from an organization's domain namespace.
- Deployment Services offer a project-based approach with education, training, and policy enactments to help ensure that companies can manage their domain catalog and email footprint upon project completion.
- Support Services offers a support team to help organizations with managing DMARC-related incidents, editorializing data reviews, and embedding DMARC into their organization's daily operations.

Boundaries of the dmarcian System

This report includes the dmarcian infrastructure and the service offerings as described above. Any other dmarcian services are not included within the scope of this report. The accompanying description references only the policies, procedures, and control activities at dmarcian, Inc. and does not include the specific policies, procedures, and control activities for any subservice organizations or vendors.

The boundaries of the dmarcian system are the specific aspects of the company's infrastructure, software, people, procedures, and data that are directly necessary to provide the DMARC Software as a Service (SaaS) offerings as described above. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Partners are not included within the boundaries of the system. The covered system specifically does not include the virtual or physical servers and systems within the Partner or end-customer environments that may be used to access, connect to, or utilize dmarcian's services. End-customer virtual machines within their provided virtual Data Center environment are the sole responsibility of the Partner and/or end-customer.



B. Principal Service Commitments and System Requirements

dmarcian designs its processes and procedures related to the DMARC Management Platform to meet its objectives for its services. Those objectives are based on the service commitments that dmarcian makes to user entities; the laws and regulations that govern the provision of its services; and the financial, operational, and compliance requirements that dmarcian has established for the services. Security, availability, and privacy commitments to user entities are documented and communicated within Terms of Service, Privacy Policy, and Partner Agreements, as well as within the description of the service offering provided online. Security, availability, and privacy commitments are standardized and include, but are not limited to, the following:

- Security and privacy principles of "Least Privilege" and "Need to Know" within the fundamental designs of the DMARC Management Platform that are designed to permit system users to access the information they need based on their role within the system while restricting them from accessing information not needed for their roles;

- The use of encryption technologies to protect customer data both at rest and in transit;

- Availability principles within the DMARC Management Platform that are designed to mitigate the impact of an availability event on operations; and

- Privacy principles within the DMARC Management Platform that are designed to collect, use, retain, access, and dispose of customer data to meet the Company's objectives and all applicable Privacy laws.

dmarcian establishes operational requirements that support the achievement of security, availability, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated within dmarcian's system policies and procedures, system design documentation, and contracts with customers. Information security and privacy policies define an organization-wide approach to how systems and data are protected.

C. Components of the System Used to Provide the Services

1. Infrastructure

dmarcian's infrastructure is deployed entirely within the Google Cloud Platform (GCP) utilizing Cloud Compute and Regional Persistent disks, Regional Snapshots, Encryption at Rest, Virtual Private Clouds isolated by application region with restricted access, minimized port exposure, and network isolation only reachable via a secure gateway. The physical access to servers is managed entirely by Google's Data Center security procedures.

dmarcian's Data Center service providers offer geographic diversity in conjunction with state-of-the-art facilities. Designed and built with reliability, security, and resiliency in mind, they provide fully redundant high-density power and cooling capacities, fully integrated UPS systems, site-wide security and fire protection systems, and access control through customer portals.

Google Cloud Platform provides the physical Data Center facility for dmarcian's Business Units. Google is responsible for physical security, environmental control, and power delivery. Multiple GCP Data Centers are utilized based on the region of the nearest dmarcian Business Unit.

2. Software

The dmarcian web application is developed with the Python programming language and is backed by PostgreSQL, RabbitMQ, Redis, and ElasticSearch components. The in-house Continuous Delivery development process involves automated testing, code reviews, automated security testing of the core code base and third-party libraries, and vulnerability scans of the servers and combined intrusion detection systems, supplemented by an automated deployment process. Application infrastructure and code are monitored in production for performance, errors, and security with alerting systems in place to notify dmarcian personnel immediately of any potential concerns. Additional supplements are in place for both abuse protection and rate limits.

3. People

dmarcian is organized to manage its services and internal operations so that client and internal needs are met and external compliance is achieved. A sociocratic organizational structure has been developed as the governance model to maximize idea circulation. dmarcian utilizes sociocratic concepts of double-linked circles, built-in transparency, and an acknowledgement of interdependence in how the company operates. Sociocratic circles are different from traditional corporate departments in that sociocratic circles execute, measure, and control their own processes while pursuing their goals. Double linking (where two people from each circle sit at the intersection between two circles) is used to connect circles so that information can flow between and across circles and to avoid situations where a single link might lead to one-way information flow or poor decision making.

dmarcian's personnel are organized by the following business units comprising all areas of customer interaction with oversight and support by Leadership.

- Corporate Business Unit (BU)
- Europe Business Unit (BU)
- Americas Business Unit (BU)
- APAC Business Unit (BU)

All personnel provide background checks and accept the Code of Conduct upon employment. Employee onboarding consists of training sessions to review all policies and procedures and receive security training. Reviews, access assessments, and training refreshers are administered on at least an annual basis.

4. Data

dmarcian's platform receives and processes DMARC aggregate and forensics reports delivered via email by DMARC report providers around the world, which provide insight on the authenticity of email sent on behalf of individual domains. This data is processed by the platform and is augmented with additional Domain Name System (DNS) data to provide insight, monitoring, and DMARC deployment planning.

A data classification scheme is defined within organizational policies and procedures to address processes for data so that it may be used and protected more efficiently. The most sensitive data classification level is confidential data which would include Personally Identifiable Information (PII), Payment Card Industry Data Security Standard (PCI DSS), authentication verifiers, contractual documents, and other legal documents.

5. Policies and Procedures

Procedures are in place to manage the security, availability, and privacy of customer data.

Changes to the System

The dmarcian Software Development Life Cycle (SDLC) follows the Continuous Delivery (CD) development flow and strives to best meet the Continuous Delivery Pipeline ideals.

The philosophy can be summarized as "test automatically, deploy small, deploy often." The goal is to maximize the flow of value delivery in the safest way possible, by deploying single changes in isolation often which will allow any unexpected side effects to be quickly reverted and traced back to a more easily identifiable piece of code.

Logical and Physical Security

dmarcian is headquartered in Brevard, NC and has offices around the world in key locations of North America, Canada, Europe, and Asia Pacific. dmarcian is a remote-first organization with a global footprint focused on attracting the top talent without being limited by geographic borders. From an IT perspective, no critical systems are housed on-site; all critical business functions are housed within the Google Cloud Platform (GCP), with controls over physical access being strictly monitored and controlled by Google.

Logical access to infrastructure is extensively restricted, network isolated, regionally segmented, and accessible only via a secure central entry point. Access to dmarcian's information systems and services is limited to those individuals who have a need-to-know. This standard is based on the principle of least privilege which states that users are only granted access necessary to complete required tasks. dmarcian's employees are granted access to various systems based on current job responsibilities and no more. User access reviews are performed on a regular basis in accordance with dmarcian's Security Review Plan.

Privacy

dmarcian follows industry standard privacy practices. Privacy obligations are outlined within dmarcian's Privacy Policy and Terms of Service, both of which are available on the dmarcian website for all customers.

A digital snapshot is taken at the time of registration to correlate the accepted version of the policy, and continued use of the platform confirms agreement. If at any point the Privacy Policy is updated, current customers are notified through the email account associated with the user while a banner may be displayed within the application or under customer notifications. All policies are reviewed at least annually.

dmarcian limits the type and amount of information collected to only what is needed to deliver service. dmarcian collects the following minimal amount of information in order to fulfill its objectives: cookies, user-submitted content, IP address information, email addresses, and email communications.

dmarcian uses this information to generate easy-to-consume reports, to collect internal metrics and analyses, and to satisfy legal processes, regulations, and requests. The information is shared with the account holder through the display of unique status reports.

Under GDPR, dmarcian acts as a sub-processor of data and upholds customers' rights to access their information and its retention, including the Right To Be Forgotten and the Transferability from the platform.

All privacy incidents are mitigated according to the Privacy Breach Complaint Policy and Procedures with oversight of the Privacy Officer in a timeframe consistent with GDPR standards.

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

The importance of controls and ethical behavior throughout dmarcian is acknowledged by management through implementation of an established control environment that sets the tone for internal activities and processes. Key aspects of the control environment include:

- Integrity and ethical values,
- A commitment to competence,
- Management's philosophy and operating style, and
- Assignment of authority and responsibility.

Integrity and Ethical Values

dmarcian has established programs and policies designed to promote and support integrity and ethical values within the organization. New employees are required to review the Employee Handbook, which covers dmarcian's culture and employees' responsibilities. Employees are required to sign a form acknowledging receipt and understanding of the contents of the Employee Handbook. The Employee Handbook is provided to all new employees and is accessible by all current employees via the internal document management system at all times.

Commitment to Competence

Prior to the offer of employment, all applicants within the Americas BU must undergo a full background check. Applicants must also sign a Proprietary Information and Invention Assignment (PIIA) agreement and read and sign the dmarcian Employee Handbook and an Employment Agreement that contains a Non-Disclosure Agreement (NDA).

The employee and supervisor work together to create a plan that provides direction and focus for a given time period. Goals include measurable performance tracks, task completion, and personal and professional development while expectations clarify the necessary competencies and behaviors to achieve those goals. One formal review is provided yearly, as well as several informal check-ins throughout the year. The company also conducts team-based 360-degree feedback and employee satisfaction surveys to encourage personal and professional growth for the entire company.

All new employees participate in onboarding training sessions to learn various aspects of dmarcian's business processes and departments, culture, and available tools. Ongoing security awareness trainings are provided for all employees and include key IT and privacy-related topics. dmarcian also encourages employees to seek out other learning opportunities.

Management's Philosophy and Operating Style

dmarcian operations proceed under direction from senior management. A Steering Committee is responsible for maintaining oversight of the organization's control environment.

2. Risk Assessment Process

dmarcian maintains a risk assessment process to identify and manage risks that could affect its ability to provide secure, reliable SaaS and subscription-based services to its users. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address and manage those risks.

Leadership's involvement in daily operations allows management to identify risks through direct personal involvement with employees, users, and vendors. Risk assessment procedures and standards are also used to provide assurance that appropriate due diligence is performed prior to the implementation of new/updated systems and that services and appropriate testing is occurring in conjunction with such projects. Risks that are considered during management's risk assessment activities include consideration of the following categories:

- Technical - Requirements, Technology, Complexity, Quality;
- Organization - Performance, Prioritization, Compliance, Resources; and
- External - Suppliers, Customers, Market conditions, Regulatory.

dmarcian performs a risk assessment at least annually and determines the likelihood and impact of identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category.

Risks are mitigated to acceptable levels based on risk criteria and ongoing assessments. For each risk mitigated, it is associated with a current control. If no control is in place, a new control is created and is monitored until the risk is reduced or eliminated. Insurance policies covering technical errors and omissions and enterprise security and privacy are in place to protect against operational and cybersecurity-related risks.

It is the policy of dmarcian to help ensure the internal controls of a vendor, maintenance and upkeep of a third-party provider's systems (if applicable), and financial condition of a third-party vendor are carefully evaluated prior to the allowance of such support services to begin, and as an on-going condition of continuing support of such products or services. Competence of a vendor for outsourced work is carefully reviewed and considered by, at a minimum, assessing the risks to dmarcian in each of the following areas, as applicable:

- Performance Risk,
- Strategic Risk,
- Financial Risk,
- Information Security and Regulatory Risk,
- Data Sensitivity and Business Risk,
- Access Risk,
- Contingency Risk,
- Volume Risk, and
- Number of Users Risk.

The Vendor Management Program details internal requirements to help ensure that all contracted vendors comply with dmarcian's information security and privacy standards.

3. Information and Communication Systems

To help align dmarcian's business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. dmarcian maintains a portal in which governance documents including policies, procedures, guidelines, and standards are hosted and are available to all staff members. The Governance documents include policies relating to Code of Conduct, data classification and protection, information security, and physical security to help govern the protection of client and company information.

dmarcian also maintains an auxiliary storage in which supplemental governance documents are available, such as but not limited to the following:

- Training materials,
- Roles and responsibilities,

- Company goals and strategies, and
- Role-specific policies and procedures.

Governance documents are considered for revision or update as well as for annual review. Employees are required to acknowledge that they agree to comply fully with all company policies and procedures, without limitation. dmarcian utilizes internal email to communicate time-sensitive changes in business processes, security, and IT operations. Regular organizational communications and status updates are distributed to staff members through the Slack platform. Corporate circle meetings are conducted on at least an annual basis to address the performance of dmarcian's service commitments.

As a result of dmarcian's sociocratic governance structure, management is involved in day-to-day operations and provides personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. Communication activities are made electronically, verbally, and through the actions of management.

Incident Response

All security incidents are retained and documented by management. Once the incident has been resolved, a Security Incident Report is created. The types of information that are logged include:

- Report Date,
- Location of Incident,
- Incident Start Date,
- Incident Notification Date,
- Identified Issue,
- Remediation Steps,
- Recommendations,
- Preventive Measures, and
- Action Items.

4. Monitoring Controls

Management monitors compliance with established policies, plans, procedures, laws, and regulations to which the company is subject. Management monitors the control environment to consider whether controls are operating as intended and that control activities are modified appropriately for changing conditions. Continuous monitoring activities are in place to assess the quality of internal control over time. Corrective actions are initiated through company meetings, department meetings, client conference calls, and informal notifications as needed. dmarcian contracts with an external audit firm on an annual basis to provide independent testing and third-party attestation of internal control relevance and adherence.

E. Description of Controls

1. Control Environment

A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.

Each US employee and contractor is subjected to a background check, including criminal and employment checks, prior to his/her start date. The Company has implemented a security awareness program to communicate the information security, availability, and privacy policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 15 days of his/her start date, and annually thereafter. The Company's new employees and contractors must sign a statement signifying that they have read, understand, and will follow the information security policies and the Company's Employee Handbook within 15 days of hire.

On an annual basis, the Corporate Circle meets to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements. On a monthly basis, departmental and management meetings are held to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business. Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities.

2. Communication and Information

The Company has provided a description of the in-scope systems and related services, including applicable information related to the boundaries of the System and its security-, availability-, and privacy-related commitments, on its website. The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail, and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.

3. Risk Assessment

The Company performs at least, an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.

4. Monitoring Activities

Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network.

On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution.

Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.

5. Control Activities

The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. Senior Management is responsible for changes to security, availability, and privacy practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users.

6. Logical and Physical Access Controls

Access to the backup tool is restricted to appropriate individuals based on job function. The backup tool is configured to automatically protect backups of the in-scope applications and related databases utilizing Advanced Encryption Standards (AESs). All cloud-hosted application data is encrypted while at rest. Direct access to the in-scope databases is restricted to appropriate users based on job function.

Valid user IDs and passwords are required to access the Company's network, in-scope application, and related databases. Password parameters for registered users of the Company's web application are configured to include a minimum password length and enforce password complexity. Password parameters for the network, the in-scope application, and the related databases are configured to meet or exceed the Company's Information Security Policy.

The ability to modify data transmission protocols is limited to appropriate users based on job function. Remote access to production systems is restricted to appropriate personnel through the use of an SSH tunnel proxy over a gateway. Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function. Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function.

Requests to add and/or modify access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases are approved by management prior to access being granted. Predefined user access profiles or roles are used to manage access to the in-scope systems based on each user’s job function. Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. The Company performs an annual review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are researched and resolved.

The Data Classification Policy, which is reviewed, updated, and approved on an annual basis by management and outlines the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information.

Customer information is purged, destroyed, or overwritten in accordance with the Company's Data Retention Policy. Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time.

Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment. A master list of system components/assets is maintained, and on an annual basis, a member of management distributes the corresponding listing of IT assets to each asset owner for review and approval. The Employee Handbook explicitly prohibits the installation of unauthorized software on laptops.

All transmissions of confidential and/or sensitive electronic information are encrypted as the default setting over public networks via Transport Layer Security (TLS) protocol. Antivirus software is in place on all workstations and Company-hosted servers related to the in-scope applications. All workstations and Company-hosted servers related to the in-scope applications are updated with current virus definitions to protect data from infection by malicious code or virus.

7. System Operations

When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved.

A Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. Backups of the in-scope databases are configured to be performed daily and hourly. The backup system is configured to alert IT personnel of any backup failures. Data restore testing is performed on an annual basis to verify the integrity of the backup data.

8. Change Management

The Company has documented a formal Change Management Policy which governs the development, acquisition, implementation, and maintenance of the in-scope systems. Version control software is in place to manage current versions of source code related to the in-scope applications and related databases.

Each change to the in-scope systems, including emergency changes, is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment. Each change to the in-scope systems, including emergency changes, must be approved by a member of management prior to promotion into the production environment. Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production.

Peer reviews and/or scans are performed on in-scope application source code to detect potential vulnerabilities prior to the release of each change into the production environment. All critical items must be remediated prior to each change being moved into the production environment. Access to promote changes into the production environment related to the in-scope systems is limited to appropriate individuals based on job function.

Automated build standards are in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and baseline configurations are stored within the configuration manager tool for roll back capability. On at least a quarterly basis, patch compliance within the development environment on virtual machines is reviewed to determine if required vendor security patches have been applied. Any identified issues are researched and resolved.

9. Risk Management

Technical errors and omissions insurance is in place to minimize the financial impact of any loss events.

On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports and in-scope ISO certifications, or the third party is subjected to continuous monitoring controls.

The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies. These commitments may contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments.

10. Availability

A monitoring tool has been implemented to monitor capacity, CPU, memory usage, and disk space and alerts are sent to IT management when predefined thresholds are met. The Company's production environment related to the in-scope applications and related databases is monitored for availability and performance on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved.

11. Privacy

The Company provides notice of its privacy practices to data subjects. The Data Privacy Officer (DPO) is responsible for helping to ensure that the notice includes the following disclosures:

- Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information;
- Policies regarding retention, sharing, disclosure, and disposal of their personal information; and
- The mechanism(s) to access, make changes to, or make inquiries regarding their personal information.

Notice is provided to the respective individuals about the Company’s privacy policies and procedures prior to personal information being collected. The Company's Privacy Policy is communicated via the Company's website, and any changes to the Company's Privacy Policy is communicated to the data subjects via the posted Privacy policy on the website. The Company has implemented a formal documented Privacy Policy and Privacy Notice which address the following:

- The purpose for collecting personal information;
- The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise and the choices available to individuals;

- The choices available to individuals with respect to the collection, use, and disclosure of personal information;
- The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained;
- The uses, retention, and disposal of personal information;
- How information may be disclosed to third parties;
- How individuals may obtain access to their personal information to review, update, and correct; and
- How compliance with the Privacy Policy is monitored and enforced.

The website User Interface (UI) screens are systematically configured to display a click button that captures and records a data subject's consent, which encompasses the acknowledgement of sub-processors used by the Company, before the data subject submits any data to the Company. For information requiring explicit consent, the Company communicates the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains consent prior to the collection of the information in accordance with the Company's Privacy Policy.

On an annual basis, the privacy staff meet to discuss relevant privacy laws and regulations to determine whether they require the Company to obtain consent. Updates to the Company's policies are made to align with any new requirements. On an annual basis, the Data Privacy Officer (DPO) reviews the Privacy Policy to help ensure that the definition of "sensitive" personal information is properly delineated and communicated to personnel. On an annual basis, privacy notices are reviewed to help ensure that personal information is used in conformity with the privacy notice, that consent is required to be received from the data subject, and that applicable laws and regulations are required to be followed.

Personal information is collected consistent with the Company's Privacy Policy. The Company uses personal information only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.

Each email request to dispose personal information is reviewed, authenticated, and processed securely within five business days. A job is configured to automatically dispose of any personal information requested to be deleted from the menu option within each individual’s personal platform account.

When an individual requests his/her personal information, the Company authenticates the individual’s identity through a username and password and, upon authentication, provides the information to the individual. If access to personal information is denied, the individual is informed of the reason, the source of the Company’s legal right to deny such access, if applicable, and the individual’s right, if any, to challenge such a denial, as specifically permitted or required by law or regulation.

Users are able to determine whether the Company maintains personal information about them through an automated system process. Upon authentication, users are provided access to their personal information maintained by the Company. Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial. When an individual requests his/her personal information, the Company provides the personal information in an understandable form, at no cost, and within five business days. Each change to personal information is logged and approved by operations personnel prior to finalization of the records. Each request to correct, amend, or append personal information is reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days.

A process is in place to address privacy inquiries, complaints, and/or disputes. Each instance is addressed, and the resolution is documented and communicated to the individual who submitted the privacy inquiry, complaint, and/or dispute.

F. Additional Information about Management's Description

The controls supporting the service organization's service commitments and system requirements based on the applicable trust services criteria are included within Section IV of this report, *Description of the Trust Services Categories, Criteria, dmarcian, Inc.'s Related Controls, and the Independent Service Auditor's Description of Tests and Results*. Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of the Company's description of its system.

G. Changes to the System During the Specified Period

There were no changes that were likely to affect report users' understanding of how the system was used to provide the service during the period from April 1, 2022 to February 28, 2023 (the "specified period").

H. System Incidents

Management did not identify any significant system incidents during the period April 1, 2022 to February 28, 2023.

I. Non-Applicable Trust Services Criteria

Common Criteria Related to Logical and Physical Access Controls		
Non-Applicable Trust Services Criteria		**dmarcian, Inc.'s Rationale**
CC 6.4	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.	All sensitive data relevant to the defined system is housed at the third-party Data Center provider. Physical access to Data Centers is outsourced to the third-party Data Center provider, Google LLC; therefore, this criterion is not applicable.
Additional Criteria for Privacy		
Non-Applicable Trust Services Criteria		**dmarcian, Inc.'s Rationale**
P 6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	dmarcian, Inc. does not disclose to or share personal information with third-parties; therefore, there is no disclosures of personal information requiring authorization. This criterion is not applicable.

J. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organization described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at this subservice organization.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organization, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Criteria Addressed
Google LLC	The Company uses Google LLC's Google Cloud Platform (GCP) for its third-party hosting of virtual servers and administrative services. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications, • Controls around the logical access of the virtual servers and administrative services; • Controls around change management of virtual servers and Google utilities supporting the Company's IT infrastructure; • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes, and • Controls around data encryption, including encrypting sensitive data at rest. In addition, the Company has identified the following control to help monitor the subservice organization: • On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations.	CC 6.1*, CC 6.4*, CC 6.7*, CC 7.5*, CC 8.1*, A 1.2*

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Criteria Addressed
	Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, in-scope ISO certifications, or the third party is subjected to continuous monitoring controls.	

* The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.

K. Complementary User Entity Controls

dmarcian, Inc.'s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Controls	Related Criteria
Each user organization is responsible for helping to ensure that access to the DMARC platform is restricted to authorized employees and that user IDs and passwords are kept confidential.	CC 6.1*
Each user organization is responsible for performing annual user access reviews to dmarcian's services and to the DMARC platform.	CC 6.2*, CC 6.3*
Each user organization is responsible for confirming that access to the DMARC platform is immediately disabled for terminated user entity personnel.	CC 6.1*, CC 6.2*, CC 6.3*
Each user organization is responsible for changing passwords to dmarcian's systems at least every 90 days.	CC 6.1*
Each user organization is responsible for deleting its personal data from dmarcian's resources when necessary.	CC 6.5*
Each user organization is responsible for notifying dmarcian of any issues, problems, or needed changes related to dmarcian's services and to the DMARC platform.	CC 2.2*, CC 2.3*

User Entity Controls	Related Criteria
Each user organization is responsible for maintaining a process to receive and respond to privacy complaints, requests for information, or requests for data disposals. Each user entity is responsible for requesting disposal of personal information by submitting a request to support@dmarcian.com or by requesting its data to be deleted via the menu option within its DMARC platform account.	P 4.3*, P 8.1*
Each user organization is responsible for communicating privacy complaints, requests for information, or requests for data disposals to dmarcian.	P 4.3*, P 8.1*
Each user organization is responsible for determining reporting requirements to data subjects and applicable authorities for any instances of a data breach.	P 6.2*, P 6.3*, P 6.6*
Each user organization is responsible for correcting, amending, or appending personal information of data subjects as required. Each user entity is responsible for requesting, correcting, amending, or appending personal information of data subjects as required.	P 5.2*
Each user organization is responsible for creating and maintaining a record of authorized disclosures of personal information and for providing data subjects with disclosure of their personal information.	P 6.2*, P 6.7*
Each user organization is responsible for reviewing the completeness and accuracy of its own registered or account-based information.	P 7.1*

* The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.

Section IV: Description of the Trust Services Categories, Criteria, dmarcian, Inc.'s Related Controls, and the Independent Service Auditor's Description of Tests and Results

A. Information Provided by FORVIS, LLP

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related controls specified by the Company in sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. If internal control is not effective at user entities, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

B. Types and Descriptions of the Tests of Operating Effectiveness

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation

In addition, as required by paragraph .36 of AT-C section 205, *Assertion-Based Examination Engagements* (AICPA, Professional Standards), when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

C. Trust Services Categories, Criteria, Control Activities, and Testing Provided by the Service Auditor

The trust services criteria relevant to security address that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the Company's ability to achieve its service commitments and system requirements.

The trust services criteria relevant to availability address that information and systems are available for operation and use to achieve the Company's service commitments and system requirements.

The trust services criteria relevant to privacy address that personal information is collected, used, retained, disclosed, and disposed to achieve the Company's service commitments and system requirements.

Control activities, test procedures, and results presented without grey shading indicate an original instance of a particular control activity, test procedure, and result within Section IV of the report. Control activities, test procedures, and results presented with a grey shading indicate that the particular control activity, test procedure, and result has been previously presented within Section IV of the report. The duplication of these items results from the requirement that each criterion stands alone and the relevance of certain control activities for multiple criteria.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC 1.1-01	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures.	Inspected the Employee Handbook to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.
CC 1.1-02	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities.	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1-03	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet.	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.1-04	The Company has implemented a security awareness program to communicate the information security, availability, and privacy policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 15 days of his/her start date, and annually thereafter.	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security, availability, and privacy policies and procedures to employees and contractors. Further, inquired of CEO to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 15 days of his/her start date.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1-05	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.
CC 1.1-06	The Company's new employees and contractors must sign a statement signifying that they have read, understand, and will follow the information security policies and the Company's Employee Handbook within 15 days of hire.	Inspected the Employee Handbook and Policy Acknowledgement Forms related to a sample of new employees and contractors to determine that each selected new employee and contractor signed a statement signifying that he/she had read, understood, and would follow the information security policies and the Company's Employee Handbook within 15 days of hire.	No exceptions noted.
CC 1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC 1.2-01	On an annual basis, the Corporate Circle meets to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	Inspected the most recent Corporate Circle meeting minutes and agenda to determine that the Corporate Circle met during the specified period to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	No exceptions noted.
CC 1.2-02	Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities.	Inspected the Organizational Chart to determine that management reviewed the Company's Organizational Chart during the specified period as part of its strategic planning process and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the CEO to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the CEO to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.
CC 1.2-03	On a monthly basis, departmental and management meetings are held to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business.	Inspected the departmental and management meeting invites and agendas related to a sample of months to determine that departmental and management meetings were held during each selected month to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business.	No exceptions noted.
CC 1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC 1.3-01	Senior Management is responsible for changes to security, availability, and privacy practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users.	Observed the security, availability, and privacy practices and commitments on the Company's intranet and website to determine that the practices and commitments were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the CEO to determine that these practices and commitments were available on the Company's intranet and website throughout the specified period.	No exceptions noted.
		Inspected the security, availability, and privacy policies to determine that Senior Management was responsible for changes to security, availability, and privacy practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security, availability, and privacy practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, e-mail, and/or contract amendment.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no changes to security, availability, and privacy practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the policy revision history used to pull the listing of changes to security, availability, and privacy practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period. Further, inquired of the CEO to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls.	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the CEO to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies . These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments.	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the CEO to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the third-party contracts related to a sample of new third parties to determine that the Chief Operating Officer reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security, availability, and privacy practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new key vendors and/or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the listing of key vendors and third parties used to pull the listing of new third parties during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no new key vendors and/or third parties during the specified period. Further, inquired of the CEO to determine that there were no new key vendors and/or third parties during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3-04	Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management reviewed the Company's Organizational Chart during the specified period as part of its strategic planning process and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the CEO to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the CEO to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.
CC 1.3-05	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.
CC 1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC 1.4-01	Each US employee and contractor is subjected to a background check, including criminal and employment checks, prior to his/her start date.	Inspected the background checks and supporting documentation related to a sample of new US employees and contractors to determine that each selected new US employee/contractor was subjected to a background check, including criminal and employment checks, prior to his/her start date.	No exceptions noted.
CC 1.4-02	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.
CC 1.4-03	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.4-04	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.4-05	The Company has implemented a security awareness program to communicate the information security, availability, and privacy policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 15 days of his/her start date, and annually thereafter. (CC 1.1-04)	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security, availability, and privacy policies and procedures to employees and contractors. Further, inquired of CEO to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 15 days of his/her start date.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.4-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.
CC 1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC 1.5-01	On a monthly basis, management performs an evaluation of internal controls, and any necessary remediation efforts are documented.	Inspected the management meeting invites and agendas related to a sample of months to determine that management performed an evaluation of internal controls during each selected month, and any necessary remediation efforts were documented.	No exceptions noted.
CC 1.5-02	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.
CC 1.5-03	Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management reviewed the Company's Organizational Chart during the specified period as part of its strategic planning process and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the CEO to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the CEO to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.
CC 1.5-04	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted.
CC 1.5-05	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.5-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC 2.1-01	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities.	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 2.1-02	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network.	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 2.1-03	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution.	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1-04	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution.	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 2.1-05	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed.	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1-06	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 2.1-07	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC 2.2-01	The Company has provided a description of the in-scope systems and related services, including applicable information related to the boundaries of the System and its security-, availability-, and privacy-related commitments, on its website.	Observed the Company's website to determine that the Company provided a description of the in-scope systems and related services on its website and that the description included applicable information related to the boundaries of the System and its security-, availability-, and privacy-related commitments. Further, inquired of the CEO to determine that a description of the in-scope systems and related services was on the Company's website throughout the specified period.	No exceptions noted.
CC 2.2-02	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.
CC 2.2-03	Senior Management is responsible for changes to security, availability, and privacy practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users. (CC 1.3-01)	Observed the security, availability, and privacy practices and commitments on the Company's intranet and website to determine that the practices and commitments were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the CEO to determine that these practices and commitments were available on the Company's intranet and website throughout the specified period.	No exceptions noted.
		Inspected the security, availability, and privacy policies to determine that Senior Management was responsible for changes to security, availability, and privacy practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security, availability, and privacy practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, e-mail, and/or contract amendment.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no changes to security, availability, and privacy practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the policy revision history used to pull the listing of changes to security, availability, and privacy practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period. Further, inquired of the CEO to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2-04	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 2.2-05	The Company has implemented a security awareness program to communicate the information security, availability, and privacy policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 15 days of his/her start date, and annually thereafter. (CC 1.1-04)	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security, availability, and privacy policies and procedures to employees and contractors. Further, inquired of CEO to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of new employees and contractors to determine that each selected new employee and contractor completed the security awareness program within 15 days of his/her start date.	No exceptions noted.
		Inspected the Security Awareness Acknowledgments related to a sample of employees and contractors to determine that each selected employee and contractor completed the security awareness program during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.
CC 2.2-07	The Company's new employees and contractors must sign a statement signifying that they have read, understand, and will follow the information security policies and the Company's Employee Handbook within 15 days of hire. (CC 1.1-06)	Inspected the Employee Handbook and Policy Acknowledgement Forms related to a sample of new employees and contractors to determine that each selected new employee and contractor signed a statement signifying that he/she had read, understood, and would follow the information security policies and the Company's Employee Handbook within 15 days of hire.	No exceptions noted.
CC 2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC 2.3-01	Senior Management is responsible for changes to security, availability, and privacy practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users. (CC 1.3-01)	Observed the security, availability, and privacy practices and commitments on the Company's intranet and website to determine that the practices and commitments were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the CEO to determine that these practices and commitments were available on the Company's intranet and website throughout the specified period.	No exceptions noted.
		Inspected the security, availability, and privacy policies to determine that Senior Management was responsible for changes to security, availability, and privacy practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security, availability, and privacy practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, e-mail, and/or contract amendment.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no changes to security, availability, and privacy practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the policy revision history used to pull the listing of changes to security, availability, and privacy practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period. Further, inquired of the CEO to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period.	No exceptions noted.
CC 2.3-02	The Company has provided a description of the in-scope systems and related services, including applicable information related to the boundaries of the System and its security-, availability-, and privacy-related commitments, on its website. (CC 2.2-01)	Observed the Company's website to determine that the Company provided a description of the in-scope systems and related services on its website and that the description included applicable information related to the boundaries of the System and its security-, availability-, and privacy-related commitments. Further, inquired of the CEO to determine that a description of the in-scope systems and related services was on the Company's website throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.3-03	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident. (CC 2.2-02)	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC 3.1-01	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 3.1-02	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.1-03	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.
CC 3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC 3.2-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.2-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, in-scope ISO certifications, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the CEO to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.2-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies. These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments. (CC 1.3-03)	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the CEO to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the third-party contracts related to a sample of new third parties to determine that the Chief Operating Officer reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security, availability, and privacy practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new key vendors and/or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the listing of key vendors and third parties used to pull the listing of new third parties during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no new key vendors and/or third parties during the specified period. Further, inquired of the CEO to determine that there were no new key vendors and/or third parties during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC 3.3-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.
CC 3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC 3.4-01	Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management reviewed the Company's Organizational Chart during the specified period as part of its strategic planning process and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the CEO to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the CEO to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.4-02	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 3.4-03	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.4-04	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, in-scope ISO certifcations, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the CEO to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC 4.1-01	Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Inspected the results from the most recent Privacy Review to determine that compliance with objectives related to privacy were reviewed and documented and that the results of the review were reported to management during the specified period. Further, inspected the results of the review and inquired of the CEO to determine that no problems were identified as a result of the review; however, that if any problems had been identified, a remediation plan would have been developed for each identified problem and that this process was in place throughout the specified period.	No exceptions noted
CC 4.1-02	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 4.1-03	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1-04	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 4.1-05	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC 4.2-01	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented.	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.
CC 4.2-02	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.2-03	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 4.2-04	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 4.2-05	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.2-06	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.
CC 4.2-07	Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented. (CC 4.1-01)	Inspected the results from the most recent Privacy Review to determine that compliance with objectives related to privacy were reviewed and documented and that the results of the review were reported to management during the specified period. Further, inspected the results of the review and inquired of the CEO to determine that no problems were identified as a result of the review; however, that if any problems had been identified, a remediation plan would have been developed for each identified problem and that this process was in place throughout the specified period.	No exceptions noted

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC 5.1-01	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 5.1-02	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 5.1-03	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1-04	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 5.1-05	Management reviews the Company's organizational structure, which is available to internal users via the Company's intranet, at least annually as part of its strategic planning process, and any needed changes are made based upon changes in reporting lines, authorities, and responsibilities. (CC 1.2-02)	Inspected the Organizational Chart to determine that management reviewed the Company's Organizational Chart during the specified period as part of its strategic planning process and that any needed changes were made based upon changes in reporting lines, authorities, and responsibilities. Further, inquired of the CEO to determine that the Organizational Chart which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Company's intranet to determine that the Organizational Chart was available to internal users via the Company's intranet. Further, inquired of the CEO to determine that the Organizational Chart was available to internal users via the Company's intranet throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1-06	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 5.1-07	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC 5.2-01	Each change to the in-scope systems, including emergency changes, is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment.	Observed the production, development, and testing environments to determine that each change to the in-scope systems was applied and tested within a development and/or testing environment separate from the production environment. Further, inquired of the CEO to determine that these environments were separate throughout the specified period.	No exceptions noted.
		Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope systems, including emergency changes, to determine that each selected change was applied and tested within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exceptions noted.
CC 5.2-02	Access to promote changes into the production environment related to the in-scope systems is limited to appropriate individuals based on job function.	Inspected the listing of users with access to promote changes into the production environment related to the in-scope systems and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 5.2-03	Each change to the in-scope systems, including emergency changes, must be approved by a member of management prior to promotion into the production environment.	Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope systems, including emergency changes, to determine that each selected change was approved by a member of management prior to promotion into the production environment.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2-04	The Company has documented a formal Change Management Policy which governs the development, acquisition, implementation, and maintenance of the in-scope systems.	Inspected the Change Management Policy to determine that the Company had documented a formal Change Management Policy which governed the development, acquisition, implementation, and maintenance of the in-scope systems. Further, inquired of the CEO to determine that the Change Management Policy which was inspected was in place throughout the specified period.	No exceptions noted.
CC 5.2-05	Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function.	Inspected the listing of users with Administrative access to the in-scope application and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 5.2-06	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function.	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listings was appropriate to have this access.	No exceptions noted.
CC 5.2-07	Valid user IDs and passwords are required to access the Company's network, in-scope application, and related databases.	Observed the authentication configurations for the network, the in-scope application, and the related databases to determine that a valid user ID and password were required to access the Company's network, in-scope application, and related databases. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2-08	On at least a quarterly basis, patch compliance within the development environment on virtual machines is reviewed to determine if required vendor security patches have been applied. Any identified issues are researched and resolved.	Inspected the patch compliance reviews to a sample of quarters to determine that patch compliance within the development environment on virtual machines was reviewed during each selected quarter to determine if required vendor security patches had been applied. Further, inspected supporting review documentation and inquired of the CEO to determine that no issues were identified as a result of the selected reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 5.2-09	Access to confidential data within the non-production environments related to the in-scope systems is restricted to appropriate users based on job function.	Inspected the listing of users with access to confidential data within the non-production environments related to the in-scope systems and the corresponding job titles for all users to determine that each user was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user was appropriate to have this access.	No exceptions noted.
CC 5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC 5.3-01	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.3-02	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 5.3-03	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 5.3-04	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.3-05	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.3-06	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-02)	Inspected the annual performance reviews related to a sample of employees to determine that a performance review was performed during the specified period for each selected employee to help ensure that his/her skill set matched his/her job responsibilities.	No exceptions noted.
CC 5.3-07	Senior Management is responsible for changes to security, availability, and privacy practices and commitments. A formal process is documented and is followed to communicate these changes to applicable internal and external users. (CC 1.3-01)	Observed the security, availability, and privacy practices and commitments on the Company's intranet and website to determine that the practices and commitments were communicated to applicable internal and external users, related parties, and vendors. Further, inquired of the CEO to determine that these practices and commitments were available on the Company's intranet and website throughout the specified period.	No exceptions noted.
		Inspected the security, availability, and privacy policies to determine that Senior Management was responsible for changes to security, availability, and privacy practices and commitments and that a formal process was documented to communicate any changes to the policies to the applicable internal and external users, related parties, and vendors.	No exceptions noted.
		Inspected the revision history and corresponding communication evidence related to a sample of changes made to the security, availability, and privacy practices and commitments to determine that each selected change was communicated to applicable internal and external users, related parties, and vendors via the Company's intranet and website, e-mail, and/or contract amendment.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no changes to security, availability, and privacy practices and commitments during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the policy revision history used to pull the listing of changes to security, availability, and privacy practices and commitments during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period. Further, inquired of the CEO to determine that there were no changes to security, availability, and privacy practices and commitments during the specified period.	No exceptions noted.
CC 5.3-08	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.3-09	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Tech Operations Department who are responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy. (CC 1.1-05)	Inspected the written job descriptions related to a sample of job positions responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Tech Operations Department who were responsible for the design, development, implementation, and operation of systems affecting system security, availability, and privacy.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1 - 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.			
CC 6.1-01	A master list of system components/assets is maintained, and reviewed and approved by a member of management on an annual basis.	Observed the master list of system components/assets to determine that a listing of system components/assets was maintained for management's use. Further, inquired of the CEO to determine that the master list of system components/assets was maintained throughout the specified period.	No exceptions noted.
		Inspected the annual IT inventory recertification documentation to determine that management reviewed and approved the listing of IT assets during the specified period.	No exceptions noted.
CC 6.1-02	Access to the backup tool is restricted to appropriate individuals based on job function.	Inspected the listing of users with access to the backup tool and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-03	The backup tool is configured to automatically protect backups of the in-scope applications and related databases utilizing Advanced Encryption Standards (AESs).	Observed the backup tool configurations to determine that the backup tool was configured to automatically protect backups of the in-scope applications and related databases with Advanced Encryption Standards (AESs). Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-04	All cloud-hosted application data is encrypted while at rest.	Observed the data encryption configurations to determine that all cloud-hosted application data was encrypted while at rest. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-05	Automated build standards are in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and baseline configurations are stored within the configuration manager tool for roll back capability.	Observed the configuration manager tool to determine that automated build standards were in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and that baseline configurations were stored within the configuration manager tool for roll back capability. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-06	Direct access to the in-scope databases is restricted to appropriate users based on job function.	Inspected the listing of users with direct access to the in-scope databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-07	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date.	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.
CC 6.1-08	Password parameters for registered users of the Company's web application are configured to include a minimum password length and enforce password complexity.	Observed the password configurations that governed user access to the Company's web application to determine that password parameters for registered users of the Company's web application were configured to include a minimum password length and enforce password complexity. Further, inquired of the New Business Analyst to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-09	Password parameters for the network, the in-scope application, and the related databases are configured to meet or exceed the Company's IT Security Program.	Observed the password configurations that governed user access to the network, the in-scope application, and the related databases, and inspected the IT Securit Program, to determine that password parameters for the network, the in-scope application, and the related databases were configured to meet or exceed the Company's IT Security Program. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-10	The ability to modify data transmission protocols is limited to appropriate users based on job function.	Inspected the listing of users with the ability to modify data transmission protocols and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-11	Remote access to production systems is restricted to appropriate personnel through the use of an SSH tunnel proxy over a gateway.	Observed the remote access authentication configurations to determine that remote access to production systems was restricted through the use of an SSH tunnel proxy over a gateway. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the listing of users with remote access to production systems and the corresponding job titles for all users to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-12	Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the in-scope application and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-13	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listings was appropriate to have this access.	No exceptions noted.
CC 6.1-14	Valid user IDs and passwords are required to access the Company's network, in-scope application, and related databases. (CC 5.2-07)	Observed the authentication configurations for the network, the in-scope application, and the related databases to determine that a valid user ID and password were required to access the Company's network, in-scope application, and related databases. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC 6.2-01	Requests to add and/or modify access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases are approved by management prior to access being granted.	Inspected the request tickets and supporting documentation related to a sample of new users granted access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases to determine that each selected new user's access was approved by his/her manager prior to access being granted.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the request tickets and supporting documentation related to a sample of access modifications to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases to determine that each selected access modification was approved by his/her manager prior to access being modified.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no access modification requests during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of access modification requests during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no access modification requests during the specified period. Further, inquired of the CEO to determine that there were no access modification requests during the specified period.	No exceptions noted.
CC 6.2-02	The Company performs an annual review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are researched and resolved.	Inspected the annual access review documentation to determine that the Company performed an annual review of access to the network, in-scope applications, and related databases during the specified period to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the CEO to determine that no issues were identified as a result of the reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.2-03	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-07)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.
CC 6.3 - 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.			
CC 6.3-01	Predefined user access profiles or roles are used to manage access to the in-scope systems based on each user's job function.	Observed the Identity Access Manager configurations to determine that the Company used predefined user access profiles or roles to manage access to the in-scope systems based on each user's job function. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the new user access request documentation related to a sample of new users granted access to the in-scope systems to determine that each selected user was granted access to predefined user profiles or roles within the in-scope systems based on his/her job function.	No exceptions noted.
CC 6.3-02	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-07)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.3-03	Requests to add and/or modify access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases are approved by management prior to access being granted. (CC 6.2-01)	Inspected the request tickets and supporting documentation related to a sample of new users granted access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases to determine that each selected new user's access was approved by his/her manager prior to access being granted.	No exceptions noted.
		Inspected the request tickets and supporting documentation related to a sample of access modifications to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases to determine that each selected access modification was approved by his/her manager prior to access being modified.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no access modification requests during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of access modification requests during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no access modification requests during the specified period. Further, inquired of the CEO to determine that there were no access modification requests during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.3-04	The Company performs an annual review of access to the network, in-scope applications, and related databases to help ensure that user access is appropriate. Any issues identified as a result of these reviews are researched and resolved. (CC 6.2-02)	Inspected the annual access review documentation to determine that the Company performed an annual review of access to the network, in-scope applications, and related databases during the specified period to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the CEO to determine that no issues were identified as a result of the reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 6.4 - 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.			
CC 6.4-01	N/A - dmarcian, Inc. is a remote-first organization with no critical systems housed on-site; all critical business functions are housed within the Google Cloud Platform (GCP), with controls over physical access being strictly monitored and controlled by Google.		
CC 6.5 - 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.			
CC 6.5-01	Customer information is purged, destroyed, or overwritten in accordance with the Company's Data Retention Policy.	Inspected the Company's Data Retention Policy and the Retention of Records Procedure to determine that the policies defined the retention period for client information and required that client information which had exceeded its retention period be purged, destroyed, or overwritten. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
		Observed the client data retention configurations to determine that client information was configured to be purged, destroyed, or overwritten in accordance with the Company's Data Retention Policy through an automatic script. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.5-02	Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time.	Inspected the Company's Data Retention Policy and the Retention of Records Procedure to determine that formal data retention and destruction standards were developed to provide guidelines for the retention of data for required periods of time and that the standards required the Company to dispose of PII data in accordance with its established retention and destruction standards. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 6.5-03	The Data Classification Policy, which is reviewed, updated, and approved on an annual basis by management and outlines the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information.	Inspected the Data Classification Policy to determine that the Data Classification Policy outlined the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information. Further, inquired of the CEO to determine that the Data Classification Policy which was inspected was in place throughout the specified period.	No exceptions noted
		Inspected the Data Classification Policy version history to determine that the Data Classification Policy was reviewed, updated, and approved by management during the specified period.	No exceptions noted
CC 6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC 6.6-01	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment.	Observed the network device (e.g., routers, switches, firewalls) configurations to determine that the devices were deployed and were maintained to detect and prevent threats to the Company's environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6-02	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.6-03	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.6-04	Access to the backup tool is restricted to appropriate individuals based on job function. (CC 6.1-02)	Inspected the listing of users with access to the backup tool and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.6-05	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listings was appropriate to have this access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6-06	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-07)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.
CC 6.6-07	Remote access to production systems is restricted to appropriate personnel through the use of an SSH tunnel proxy over a gateway. (CC 6.1-11)	Observed the remote access authentication configurations to determine that remote access to production systems was restricted through the use of an SSH tunnel proxy over a gateway. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the listing of users with remote access to production systems and the corresponding job titles for all users to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.7 - 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.			
CC 6.7-01	All transmissions of confidential and/or sensitive electronic information are encrypted as the default setting over public networks via Transport Layer Security (TLS) protocol.	Observed the transmission configurations to determine that all transmissions of confidential information and/or sensitive electronic information were encrypted as the default setting over public networks via TLS protocol. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.7-02	Access to the backup tool is restricted to appropriate individuals based on job function. (CC 6.1-02)	Inspected the listing of users with access to the backup tool and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.7-03	The backup tool is configured to automatically protect backups of the in-scope applications and related databases utilizing Advanced Encryption Standards (AESs). (CC 6.1-03)	Observed the backup tool configurations to determine that the backup tool was configured to automatically protect backups of the in-scope applications and related databases with Advanced Encryption Standards (AESs). Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.7-04	Direct access to the in-scope databases is restricted to appropriate users based on job function. (CC 6.1-06)	Inspected the listing of users with direct access to the in-scope databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.7-05	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listings was appropriate to have this access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.7-06	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-07)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.
CC 6.7-07	Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the in-scope application and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC 6.8-01	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production.	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8-02	Peer reviews and/or scans are performed on in-scope application source code to detect potential vulnerabilities prior to the release of each change into the production environment. All critical items must be remediated prior to each change being moved into the production environment.	Inspected the peer review and/or source code scan results and the corresponding change tickets related to a sample of in-scope application source code changes to determine that a peer review and/or scan was performed prior to the release of each selected in-scope application source code change into the production environment. Further, inspected the peer review and/or source code scan results and the corresponding remediation documentation, if applicable, for each selected in-scope application source code change to determine that each critical item identified within the scans was remediated prior to the selected change being moved into the production environment.	No exceptions noted.
CC 6.8-03	The Employee Handbook explicitly prohibits the installation of unauthorized software on laptops.	Inspected the Employee Handbook to determine that the Employee Handbook explicitly prohibited the installation of unauthorized software on laptops. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.
CC 6.8-04	Access to promote changes into the production environment related to the in-scope systems is limited to appropriate individuals based on job function. (CC 5.2-02)	Inspected the listing of users with access to promote changes into the production environment related to the in-scope systems and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8-05	Automated build standards are in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and baseline configurations are stored within the configuration manager tool for roll back capability. (CC 6.1-05)	Observed the configuration manager tool to determine that automated build standards were in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and that baseline configurations were stored within the configuration manager tool for roll back capability. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.8-06	Administrative access to the in-scope application and related databases is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the in-scope application and related databases and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.8-07	Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listings of users with Administrative access to the network and in-scope utilities, including access to firewalls and intrusion detection devices, and the corresponding job titles for all users on the listings to determine that each user on the listings was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listings was appropriate to have this access.	No exceptions noted.
CC 6.8-08	Access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases is removed or disabled within five business days of the employee's/contractor's termination date. (CC 6.1-07)	Inspected the termination tickets and supporting documentation related to a sample of terminated employees and contractors to determine that each selected terminated employee's or contractor's access to the network, to the in-scope utilities, to the in-scope applications, and/or to the related databases was removed or disabled within five business days of the employee's/contractor's termination date.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.1 - 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.			
CC 7.1-01	A monitoring tool has been implemented to monitor capacity, CPU, memory usage, and disk space and alerts are sent to IT management when predefined thresholds are met.	Observed the monitoring system configurations to determine that a monitoring tool had been implemented to monitor capacity, CPU, memory usage, and disk space, and that alerts were automatically sent to IT management when predefined thresholds were met. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.1-02	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production. (CC 6.8-01)	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.1-03	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.1-04	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.2 - 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.			
CC 7.2-01	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production. (CC 6.8-01)	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.2-02	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.2-03	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.3 - 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.			
CC 7.3-01	The Company's production environment related to the in-scope applications and related databases is monitored for availability and performance on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved.	Observed the monitoring tool configurations for the production environment related to the in-scope applications and related databases to determine that the Company's production environment was monitored for availability and performance on an ongoing basis and that IT personnel were automatically notified in the event of an incident. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the resolution documentation related to a sample of actionable availability incidents to determine that each selected incident was researched and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no actionable availability and performance incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the system-generated listing of actionable risks during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no actionable availability and performance incidents during the specified period. Further, inquired of the CEO to determine that there were no actionable availability and performance incidents during the specified period.	No exceptions noted.
CC 7.3-02	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved.	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.
CC 7.3-03	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production. (CC 6.8-01)	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.3-04	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-05	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.3-06	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.3-07	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-08	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-09	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-10	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident. (CC 2.2-02)	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-11	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.
CC 7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC 7.4-01	Data restore testing is performed on an annual basis to verify the integrity of the backup data.	Inspected the results from the most recent annual data restore test to determine that data restore testing was performed during the specified period to verify the integrity of the backup data. Further, inspected the results of the most recent annual data restore test and inquired of the CEO to determine that no issues were identified during the annual data restore test; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.4-02	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production. (CC 6.8-01)	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.4-03	Intrusion Detection Systems (IDSs) are configured to provide continuous monitoring of the Company's network and early identification of potential security breaches, security threats, and unusual system activities. (CC 2.1-01)	Observed the IDS configurations to determine that the IDSs were configured to provide continuous monitoring of the Company's network to identify potential security breaches, security threats, and unusual system activities and to send alert notifications to the IT Security Team when specific predefined conditions were met. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.4-04	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 7.4-05	On a monthly basis, scans are performed to detect instances of malicious applications and vulnerabilities within the production environment. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-03)	Inspected the scans related to a sample of months to determine that scans were performed to detect instances of malicious applications and vulnerabilities within the production environment during each selected month. Further, inspected the scan results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-06	On an annual basis, internal and external network vulnerability scanning is performed to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked until resolution. (CC 2.1-04)	Inspected the most recent internal and external network scanning results to determine that internal and external network vulnerability scanning was performed to detect new and unknown vulnerabilities during the specified period. Further, inspected the test results and inquired of the CEO to determine that no critical/high vulnerabilities were identified during the scans; however, that if any critical/high vulnerabilities had been identified, each vulnerability would have been tracked until resolution and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.4-07	The Company's production environment related to the in-scope applications and related databases is monitored for availability and performance on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved. (CC 7.3-01)	Observed the monitoring tool configurations for the production environment related to the in-scope applications and related databases to determine that the Company's production environment was monitored for availability and performance on an ongoing basis and that IT personnel were automatically notified in the event of an incident. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the resolution documentation related to a sample of actionable availability incidents to determine that each selected incident was researched and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no actionable availability and performance incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the system-generated listing of actionable risks during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no actionable availability and performance incidents during the specified period. Further, inquired of the CEO to determine that there were no actionable availability and performance incidents during the specified period.	No exceptions noted.
CC 7.4-08	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.
CC 7.4-09	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved. (CC 7.3-02)	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-10	The Company has implemented a formal written IT Security Program, Incident Management Procedure, and Privacy Policy which collectively address the security, availability, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet. (CC 1.1-03)	Observed the Company's intranet to determine that the IT Security Program, Incident Management Procedure, and Privacy Policy were posted on the Company's intranet. Further, inquired of the Data Protection Officer to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the IT Security Program, Incident Management Procedure, and Privacy Policy to determine that these policies collectively addressed the security, availability, and privacy of the system; covered the escalation process for security breaches and other incidents; and were reviewed and approved by management during the specified period. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-11	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident. (CC 2.2-02)	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-12	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.
CC 7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC 7.5-01	A Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved.	Inspected the Business Continuity and Disaster Recovery Plan and related testing results to determine that a Business Continuity and Disaster Recovery Plan was documented and was tested during the specified period. Further, inspected the test results and inquired of the CEO to determine that no issues were identified during the testing of the Plan; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.5-02	Backups of the in-scope databases are configured to be performed daily and hourly. The backup system is configured to alert IT personnel of any backup failures.	Observed the incremental backup configurations for the in-scope databases to determine that backups of the in-scope databases were configured to be performed daily and hourly and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.5-03	The Company's production environment related to the in-scope applications and related databases is monitored for availability and performance on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved. (CC 7.3-01)	Observed the monitoring tool configurations for the production environment related to the in-scope applications and related databases to determine that the Company's production environment was monitored for availability and performance on an ongoing basis and that IT personnel were automatically notified in the event of an incident. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the resolution documentation related to a sample of actionable availability incidents to determine that each selected incident was researched and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no actionable availability and performance incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the system-generated listing of actionable risks during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no actionable availability and performance incidents during the specified period. Further, inquired of the CEO to determine that there were no actionable availability and performance incidents during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.5-04	Data restore testing is performed on an annual basis to verify the integrity of the backup data. (CC 7.4-01)	Inspected the results from the most recent annual data restore test to determine that data restore testing was performed during the specified period to verify the integrity of the backup data. Further, inspected the results of the most recent annual data restore test and inquired of the CEO to determine that no issues were identified during the annual data restore test; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.5-05	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.
CC 7.5-06	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved. (CC 7.3-02)	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.5-07	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident. (CC 2.2-02)	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC 8.1-01	Version control software is in place to manage current versions of source code related to the in-scope applications and related databases.	Observed the version control software and related code repositories to determine that version control software was in place to manage the current versions of source code related to the in-scope applications and related databases. Further, inquired of the Technical Operations Manager to determine that the version control software was in place throughout the specified period.	No exceptions noted.
CC 8.1-02	A master list of system components/assets is maintained, and reviewed and approved by a member of management on an annual basis. (CC 6.1-01)	Observed the master list of system components/assets to determine that a listing of system components/assets was maintained for management's use. Further, inquired of the CEO to determine that the master list of system components/assets was maintained throughout the specified period.	No exceptions noted.
		Inspected the annual IT inventory recertification documentation to determine that management reviewed and approved the listing of IT assets during the specified period.	No exceptions noted.
CC 8.1-03	Automated alerts are sent to management when changes are implemented into the production environment. Audit logging is enabled on the production environment to provide management with an audit trail in the event of any issues within production. (CC 6.8-01)	Observed the alerting configurations to determine that automated alerts were sent to management when changes were implemented into the production environment. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Observed the logging configurations to determine that audit logging was enabled on the production environment to provide management with an audit trail in the event of any issues in production. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1-04	Each change to the in-scope systems, including emergency changes, is applied and tested within development and/or testing environments which are separate from the production environment prior to migration into the production environment. (CC 5.2-01)	Observed the production, development, and testing environments to determine that each change to the in-scope systems was applied and tested within a development and/or testing environment separate from the production environment. Further, inquired of the CEO to determine that these environments were separate throughout the specified period.	No exceptions noted.
		Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope systems, including emergency changes, to determine that each selected change was applied and tested within a development and/or testing environment separate from the production environment prior to migration into the production environment.	No exceptions noted.
CC 8.1-05	Access to promote changes into the production environment related to the in-scope systems is limited to appropriate individuals based on job function. (CC 5.2-02)	Inspected the listing of users with access to promote changes into the production environment related to the in-scope systems and the corresponding job titles for all users on the listing to determine that each user on the listing was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 8.1-06	Each change to the in-scope systems, including emergency changes, must be approved by a member of management prior to promotion into the production environment. (CC 5.2-03)	Inspected the change tickets and supporting documentation related to a sample of changes to the in-scope systems, including emergency changes, to determine that each selected change was approved by a member of management prior to promotion into the production environment.	No exceptions noted.
CC 8.1-07	The Company has documented a formal Change Management Policy which governs the development, acquisition, implementation, and maintenance of the in-scope systems. (CC 5.2-04)	Inspected the Change Management Policy to determine that the Company had documented a formal Change Management Policy which governed the development, acquisition, implementation, and maintenance of the in-scope systems. Further, inquired of the CEO to determine that the Change Management Policy which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1-08	Peer reviews and/or scans are performed on in-scope application source code to detect potential vulnerabilities prior to the release of each change into the production environment. All critical items must be remediated prior to each change being moved into the production environment. (CC 6.8-02)	Inspected the peer review and/or source code scan results and the corresponding change tickets related to a sample of in-scope application source code changes to determine that a peer review and/or scan was performed prior to the release of each selected in-scope application source code change into the production environment. Further, inspected the peer review and/or source code scan results and the corresponding remediation documentation, if applicable, for each selected in-scope application source code change to determine that each critical item identified within the scans was remediated prior to the selected change being moved into the production environment.	No exceptions noted.
CC 8.1-09	Automated build standards are in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and baseline configurations are stored within the configuration manager tool for roll back capability. (CC 6.1-05)	Observed the configuration manager tool to determine that automated build standards were in place to provide consistency when building, implementing, and upgrading servers supporting the in-scope applications and related databases, and that baseline configurations were stored within the configuration manager tool for roll back capability. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 8.1-10	On at least a quarterly basis, patch compliance within the development environment on virtual machines is reviewed to determine if required vendor security patches have been applied. Any identified issues are researched and resolved. (CC 5.2-08)	Inspected the patch compliance reviews to a sample of quarters to determine that patch compliance within the development environment on virtual machines was reviewed during each selected quarter to determine if required vendor security patches had been applied. Further, inspected supporting review documentation and inquired of the CEO to determine that no issues were identified as a result of the selected reviews; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 8.1-11	Access to confidential data within the non-production environments related to the in-scope systems is restricted to appropriate users based on job function. (CC 5.2-09)	Inspected the listing of users with access to confidential data within the non-production environments related to the in-scope systems and the corresponding job titles for all users to determine that each user was appropriate to have this access based on job function. Further, inquired of the CEO to determine that each user was appropriate to have this access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC 9.1-01	Technical errors and omissions insurance is in place to minimize the financial impact of any loss events.	Inspected the technical errors and omissions insurance policy to determine that technical errors and omissions insurance was in place to minimize the financial impact of any loss events. Further, inquired of the CEO to determine that the insurance policy which was inspected was in place throughout the specified period.	No exceptions noted.
CC 9.1-02	A Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. (CC 7.5-01)	Inspected the Business Continuity and Disaster Recovery Plan and related testing results to determine that a Business Continuity and Disaster Recovery Plan was documented and was tested during the specified period. Further, inspected the test results and inquired of the CEO to determine that no issues were identified during the testing of the Plan; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 9.1-03	Backups of the in-scope databases are configured to be performed daily and hourly. The backup system is configured to alert IT personnel of any backup failures. (CC 7.5-02)	Observed the incremental backup configurations for the in-scope databases to determine that backups of the in-scope databases were configured to be performed daily and hourly and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1-04	Data restore testing is performed on an annual basis to verify the integrity of the backup data. (CC 7.4-01)	Inspected the results from the most recent annual data restore test to determine that data restore testing was performed during the specified period to verify the integrity of the backup data. Further, inspected the results of the most recent annual data restore test and inquired of the CEO to determine that no issues were identified during the annual data restore test; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 9.1-05	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC 9.2-01	The Company performs an annual risk assessment which includes the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to the security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system. As part of the annual risk assessment process, these threats are formally assessed, and mitigation strategies are documented and revised as needed. (CC 2.1-05)	Inspected the Annual Risk Assessment to determine that the Company performed a risk assessment during the specified period which included the identification and assessment of applicable laws and regulations (including environmental, regulatory, and technological changes, and threats related to fraud), defined commitments, service-level agreements, other contractual requirements, and potential threats to security (including threats related to the use of vendors and other third parties providing goods and services), availability, and privacy of the system and that as part of the risk assessment process, these threats were formally assessed and mitigation strategies were documented and revised as needed.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2-02	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the CEO to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security, Availability, and Privacy Trust Services Categories			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2-03	The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies . These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments. (CC 1.3-03)	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the CEO to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the third-party contracts related to a sample of new third parties to determine that the Chief Operating Officer reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security, availability, and privacy practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new key vendors and/or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the listing of key vendors and third parties used to pull the listing of new third parties during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no new key vendors and/or third parties during the specified period. Further, inquired of the CEO to determine that there were no new key vendors and/or third parties during the specified period.	No exceptions noted.

AVAILABILITY CATEGORY: Additional Criteria for Availability			
CRITERIA GROUP 1: Additional Criteria for Availability			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
A 1.1 - 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.			
A 1.1-01	A monitoring tool has been implemented to monitor capacity, CPU, memory usage, and disk space and alerts are sent to IT management when predefined thresholds are met. (CC 7.1-01)	Observed the monitoring system configurations to determine that a monitoring tool had been implemented to monitor capacity, CPU, memory usage, and disk space, and that alerts were automatically sent to IT management when predefined thresholds were met. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
A 1.1-02	The Company's production environment related to the in-scope applications and related databases is monitored for availability and performance on an ongoing basis, and IT personnel are automatically notified in the event of an incident. Any actionable incidents are researched and resolved. (CC 7.3-01)	Observed the monitoring tool configurations for the production environment related to the in-scope applications and related databases to determine that the Company's production environment was monitored for availability and performance on an ongoing basis and that IT personnel were automatically notified in the event of an incident. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the resolution documentation related to a sample of actionable availability incidents to determine that each selected incident was researched and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no actionable availability and performance incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

AVAILABILITY CATEGORY: Additional Criteria for Availability			
CRITERIA GROUP 1: Additional Criteria for Availability			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the system-generated listing of actionable risks during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting system-generated listing to determine that there were no actionable availability and performance incidents during the specified period. Further, inquired of the CEO to determine that there were no actionable availability and performance incidents during the specified period.	No exceptions noted.
A 1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A 1.2-01	Backups of the in-scope databases are configured to be performed daily and hourly. The backup system is configured to alert IT personnel of any backup failures. (CC 7.5-02)	Observed the incremental backup configurations for the in-scope databases to determine that backups of the in-scope databases were configured to be performed daily and hourly and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
A 1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A 1.3-01	A Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. (CC 7.5-01)	Inspected the Business Continuity and Disaster Recovery Plan and related testing results to determine that a Business Continuity and Disaster Recovery Plan was documented and was tested during the specified period. Further, inspected the test results and inquired of the CEO to determine that no issues were identified during the testing of the Plan; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

AVAILABILITY CATEGORY: Additional Criteria for Availability			
CRITERIA GROUP 1: Additional Criteria for Availability			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
A 1.3-02	Data restore testing is performed on an annual basis to verify the integrity of the backup data. (CC 7.4-01)	Inspected the results from the most recent annual data restore test to determine that data restore testing was performed during the specified period to verify the integrity of the backup data. Further, inspected the results of the most recent annual data restore test and inquired of the CEO to determine that no issues were identified during the annual data restore test; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 1: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 1.1 - The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
P 1.1-01	The Company provides notice of its privacy practices to data subjects. The Data Privacy Officer (DPO) is responsible for helping to ensure that the notice includes the following disclosures: • Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information; • Policies regarding retention, sharing, disclosure, and disposal of their personal information; and • The mechanism(s) to access, make changes to, or make inquiries regarding their personal information.	Inspected the Privacy Policy to determine that the Data Privacy Officer (DPO) was responsible for helping to ensure that the notice included the following disclosures: • Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information; • Policies regarding retention, sharing, disclosure, and disposal of their personal information; and • The mechanism(s) to access, make changes to, or make inquiries regarding their personal information. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Privacy Policy on the Company's external website to determine that the Privacy Policy was available to all individuals. Further, inquired of the Data Protection Officer to determine that Privacy Policy was available on the Company's external website throughout the specified period.	No exceptions noted.
P 1.1-02	Notice is provided to the respective individuals about the Company's privacy policies and procedures prior to personal information being collected.	Inspected the privacy notice to determine that the notice provided to individuals included information about the Company's privacy policies and procedures. Further, inquired of the Data Protection Officer to determine that the privacy policies which were inspected were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 1: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Observed the Company's external website to determine that notice was provided to individuals about the Company's privacy policies and procedures prior to personal information being collected. Further, inquired of the Data Protection Officer to determine that this process was in place throughout the specified period.	No exceptions noted.
P 1.1-03	The Company's Privacy Policy is communicated via the Company's website, and any changes to the Company's Privacy Policy is communicated to the data subjects via the posted Privacy policy on the website.	Observed the Company's website to determine that the Company's Privacy Policy was communicated via the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the Privacy Policy revision history and observed the Company's website to determine that any change to the Company's Privacy Policy was communicated to data subjects by the updated policy posted on the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 1: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 1.1-04	The Company has implemented a formal documented Privacy Policy and Privacy Notice which address the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced.	Inspected the Company's Privacy Policy and Privacy Notice to determine that the Company had implemented a formal documented Privacy Policy and Privacy Notice which addressed the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically required otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 2: Privacy Criteria Related to Choice and Consent			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 2.1 - The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
P 2.1-01	The website User Interface (UI) screens are systematically configured to display a click button that captures and records a data subject's consent, which encompasses the acknowledgement of sub-processors used by the Company, before the data subject submits any data to the Company.	Observed the website configurations to determine that the website User Interface (UI) screens were systematically configured to display a click button that captured and recorded a data subject's consent, which encompassed the acknowledgement of sub-processors used by the Company, before the data subject submitted any data to the Company. Further, inquired of the Data Protection Officer to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 2.1-02	For information requiring explicit consent, the Company communicates the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains consent prior to the collection of the information in accordance with the Company's Privacy Policy.	Inspected the Privacy Policy to determine that, for information requiring explicit consent, the Company communicated the need for consent, as well as the consequences of a failure to provide consent for the request for personal information. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the click-through agreement configurations to determine that the dmarcian System was configured to communicate the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, and was configured to obtain consent prior to the collection of the information. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 2: Privacy Criteria Related to Choice and Consent			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 2.1-03	On an annual basis, the privacy staff meet to discuss relevant privacy laws and regulations to determine whether they require the Company to obtain consent. Updates to the Company's policies are made to align with any new requirements.	Inspected the results from the most recent Privacy Review to determine that the privacy staff met during the specified period to discuss relevant privacy laws and regulations to determine whether they required the Company to obtain consent, and updates to the Company's policies were made to align with any new requirements.	No exceptions noted.
P 2.1-04	On an annual basis, the Data Privacy Officer (DPO) reviews the Privacy Policy to help ensure that the definition of "sensitive" personal information is properly delineated and communicated to personnel.	Inspected the results from the most recent Privacy Review and inspected the Privacy Policy to determine that the Data Privacy Officer (DPO) reviewed the Privacy Policy during the specified period to help ensure that the definition of "sensitive" personal information was properly delineated and communicated to personnel.	No exceptions noted.
P 2.1-05	The Company provides notice of its privacy practices to data subjects. The Data Privacy Officer (DPO) is responsible for helping to ensure that the notice includes the following disclosures: • Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information; • Policies regarding retention, sharing, disclosure, and disposal of their personal information; and • The mechanism(s) to access, make changes to, or make inquiries regarding their personal information. (P 1.1-01)	Inspected the Privacy Policy to determine that the Data Privacy Officer (DPO) was responsible for helping to ensure that the notice included the following disclosures: • Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information; • Policies regarding retention, sharing, disclosure, and disposal of their personal information; and • The mechanism(s) to access, make changes to, or make inquiries regarding their personal information. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.
		Observed the Privacy Policy on the Company's external website to determine that the Privacy Policy was available to all individuals. Further, inquired of the Data Protection Officer to determine that Privacy Policy was available on the Company's external website throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 2: Privacy Criteria Related to Choice and Consent			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 2.1-06	Notice is provided to the respective individuals about the Company's privacy policies and procedures prior to personal information being collected. (P 1.1-02)	Inspected the privacy notice to determine that the notice provided to individuals included information about the Company's privacy policies and procedures. Further, inquired of the Data Protection Officer to determine that the privacy policies which were inspected were in place throughout the specified period.	No exceptions noted.
		Observed the Company's external website to determine that notice was provided to individuals about the Company's privacy policies and procedures prior to personal information being collected. Further, inquired of the Data Protection Officer to determine that this process was in place throughout the specified period.	No exceptions noted.
P 2.1-07	The Company's Privacy Policy is communicated via the Company's website, and any changes to the Company's Privacy Policy is communicated to the data subjects via the posted Privacy policy on the website. (P 1.1-03)	Observed the Company's website to determine that the Company's Privacy Policy was communicated via the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the Privacy Policy revision history and observed the Company's website to determine that any change to the Company's Privacy Policy was communicated to data subjects by the updated policy posted on the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 2: Privacy Criteria Related to Choice and Consent			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 2.1-08	The Company has implemented a formal documented Privacy Policy and Privacy Notice which address the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced. (P 1.1-04)	Inspected the Company's Privacy Policy and Privacy Notice to determine that the Company had implemented a formal documented Privacy Policy and Privacy Notice which addressed the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically required otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 3: Privacy Criteria Related to Collection			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 3.1 - Personal information is collected consistent with the entity's objectives related to privacy.			
P 3.1-01	Personal information is collected consistent with the Company's Privacy Policy.	Observed the dmarcian System configurations related to the personal information collection process and inspected the Company's Privacy Policy to determine that the dmarcian System was configured to limit the collection of personal information consistent with the Company's Privacy Policy. Further, inquired of the Data Protection Officer to determine that these configurations and the Privacy Policy were in place throughout the specified period.	No exceptions noted.
P 3.2 - For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
P 3.2-01	The website User Interface (UI) screens are systematically configured to display a click button that captures and records a data subject's consent, which encompasses the acknowledgement of sub-processors used by the Company, before the data subject submits any data to the Company. (P 2.1-01)	Observed the website configurations to determine that the website User Interface (UI) screens were systematically configured to display a click button that captured and recorded a data subject's consent, which encompassed the acknowledgement of sub-processors used by the Company, before the data subject submitted any data to the Company. Further, inquired of the Data Protection Officer to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 3.2-02	For information requiring explicit consent, the Company communicates the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains consent prior to the collection of the information in accordance with the Company's Privacy Policy. (P 2.1-02)	Inspected the Privacy Policy to determine that, for information requiring explicit consent, the Company communicated the need for consent, as well as the consequences of a failure to provide consent for the request for personal information. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 3: Privacy Criteria Related to Collection			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Observed the click-through agreement configurations to determine that the dmarcian System was configured to communicate the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, and was configured to obtain consent prior to the collection of the information. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 4: Privacy Criteria Related to Use, Retention, and Disposal			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 4.1 - The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P 4.1-01	The Company uses personal information only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.	Observed the information collection process related to the in-scope applications to determine that explicit consent was obtained from individuals prior to personal information being collected and that an individual could not circumvent the notice/consent process. In addition, observed the collection process configurations to determine that the individual's preferences expressed in his/her consent were confirmed and automatically implemented. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the Company's Privacy Policy and contractual agreements related to a sample of third parties with whom personal information was shared to determine that each selected third party's use of the personal information was limited to data matching as specified within the Company's Privacy Policy.	No exceptions noted.
P 4.1-02	On an annual basis, privacy notices are reviewed to help ensure that personal information is used in conformity with the privacy notice, that consent is required to be received from the data subject, and that applicable laws and regulations are required to be followed.	Inspected the results from the most recent Privacy Review and inspected the Privacy Policy to determine that privacy notices were reviewed during the specified period to help ensure that personal information was used in conformity with the privacy notice, that consent was required to be received from the data subject, and that applicable laws and regulations were required to be followed.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 4: Privacy Criteria Related to Use, Retention, and Disposal			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 4.2 - The entity retains personal information consistent with the entity's objectives related to privacy.			
P 4.2-01	Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time. (CC 6.5-02)	Inspected the Company's Data Retention Policy and the Retention of Records Procedure to determine that formal data retention and destruction standards were developed to provide guidelines for the retention of data for required periods of time and that the standards required the Company to dispose of PII data in accordance with its established retention and destruction standards. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
P 4.2-02	Backups of the in-scope databases are configured to be performed daily and hourly. The backup system is configured to alert IT personnel of any backup failures. (CC 7.5-02)	Observed the incremental backup configurations for the in-scope databases to determine that backups of the in-scope databases were configured to be performed daily and hourly and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 4.2-03	Data restore testing is performed on an annual basis to verify the integrity of the backup data. (CC 7.4-01)	Inspected the results from the most recent annual data restore test to determine that data restore testing was performed during the specified period to verify the integrity of the backup data. Further, inspected the results of the most recent annual data restore test and inquired of the CEO to determine that no issues were identified during the annual data restore test; however, that if any issues had been identified, each issue would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 4: Privacy Criteria Related to Use, Retention, and Disposal			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 4.2-04	The Data Classification Policy, which is reviewed, updated, and approved on an annual basis by management and outlines the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information. (CC 6.5-03)	Inspected the Data Classification Policy to determine that the Data Classification Policy outlined the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information. Further, inquired of the CEO to determine that the Data Classification Policy which was inspected was in place throughout the specified period.	No exceptions noted
		Inspected the Data Classification Policy version history to determine that the Data Classification Policy was reviewed, updated, and approved by management during the specified period.	No exceptions noted
P 4.3 - The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P 4.3-01	Each e-mail request to dispose personal information is reviewed, authenticated, and processed securely within five business days.	Inspected the e-mail requests and supporting disposal documentation related to a sample of e-mail requests to dispose of personal information to determine that each selected e-mail request to dispose personal information was reviewed, authenticated, and processed securely within five business days.	No exceptions noted.
P 4.3-02	A job is configured to automatically dispose of any personal information requested to be deleted from the menu option within each individual's personal platform account.	Observed the automated job script and menu options to determine that a job was configured to automatically dispose of any personal information requested to be deleted from the menu option within each individual's personal platform account. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 4: Privacy Criteria Related to Use, Retention, and Disposal			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 4.3-03	Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time. (CC 6.5-02)	Inspected the Company's Data Retention Policy and the Retention of Records Procedure to determine that formal data retention and destruction standards were developed to provide guidelines for the retention of data for required periods of time and that the standards required the Company to dispose of PII data in accordance with its established retention and destruction standards. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
P 4.3-04	The Data Classification Policy, which is reviewed, updated, and approved on an annual basis by management and outlines the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information. (CC 6.5-03)	Inspected the Data Classification Policy to determine that the Data Classification Policy outlined the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information, as well as the identification of related processes, systems, and third parties involved in the handling of such information. Further, inquired of the CEO to determine that the Data Classification Policy which was inspected was in place throughout the specified period.	No exceptions noted
		Inspected the Data Classification Policy version history to determine that the Data Classification Policy was reviewed, updated, and approved by management during the specified period.	No exceptions noted

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 5.1 - The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
P 5.1-01	When an individual requests his/her personal information, the Company authenticates the individual's identity through a username and password and, upon authentication, provides the information to the individual.	Observed the system configurations related to the personal information request process to determine that the dmarcian System was configured to authenticate an individual's identity through a username and password and that, upon authentication, the dmarcian System was configured to provide the information to the individual. Further, inquired of the Data Protection Officer to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 5.1-02	If access to personal information is denied, the individual is informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation.	Inspected the tickets and supporting documentation related to a sample of denied information requests to determine that the individual was informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation, for each selected denied information request.	No exceptions noted.
P 5.1-03	Users are able to determine whether the Company maintains personal information about them through an automated system process. Upon authentication, users are provided access to their personal information maintained by the Company.	Observed the automated dmarcian System configurations to determine that users were able to determine whether the Company maintained personal information about them through an automated system process. Further, observed the automated system configurations to determine that, upon authentication, users were provided access to their personal information maintained by the Company. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 5.1-04	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial.	Inspected supporting documentation related to a sample of denied correction of personal information requests to determine that each respective individual was informed, in writing, about the reason his/her request for correction of personal information was denied and how he/she could appeal the denial.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for correction of personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests made by individuals pertaining to the correction of personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for correction of personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for correction of personal information during the specified period.	No exceptions noted.
P 5.1-05	When an individual requests his/her personal information, the Company provides the personal information in an understandable form, at no cost, and within five business days.	Inspected the personal information requests and supporting documentation related to a sample of requests by individuals for their personal information to determine that the Company provided the personal information in an understandable form, at no cost, and within five business days for each selected request.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of requests for an individual's personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for personal information during the specified period.	No exceptions noted.
P 5.1-06	Each request to correct, amend, or append personal information is reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days.	Inspected the log and approvals related to a sample of requests to correct, amend, or append personal information to determine that each selected request was reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests to correct, amend, or append personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests to correct, amend, or append personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests to correct, amend, or append personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests to correct, amend, or append personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 5.2 - The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
P 5.2-01	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial. (P 5.1-04)	Inspected supporting documentation related to a sample of denied correction of personal information requests to determine that each respective individual was informed, in writing, about the reason his/her request for correction of personal information was denied and how he/she could appeal the denial.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for correction of personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests made by individuals pertaining to the correction of personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for correction of personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for correction of personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 5.2-02	When an individual requests his/her personal information, the Company provides the personal information in an understandable form, at no cost, and within five business days. (P 5.1-05)	Inspected the personal information requests and supporting documentation related to a sample of requests by individuals for their personal information to determine that the Company provided the personal information in an understandable form, at no cost, and within five business days for each selected request.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests for an individual's personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for personal information during the specified period.	No exceptions noted.
P 5.2-03	Each request to correct, amend, or append personal information is reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days. (P 5.1-06)	Inspected the log and approvals related to a sample of requests to correct, amend, or append personal information to determine that each selected request was reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests to correct, amend, or append personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 5: Privacy Criteria Related to Access			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of requests to correct, amend, or append personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests to correct, amend, or append personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests to correct, amend, or append personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.1 - The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
P 6.1-01	The website User Interface (UI) screens are systematically configured to display a click button that captures and records a data subject's consent, which encompasses the acknowledgement of sub-processors used by the Company, before the data subject submits any data to the Company. (P 2.1-01)	Observed the website configurations to determine that the website User Interface (UI) screens were systematically configured to display a click button that captured and recorded a data subject's consent, which encompassed the acknowledgement of sub-processors used by the Company, before the data subject submitted any data to the Company. Further, inquired of the Data Protection Officer to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 6.1-02	The Company's Privacy Policy is communicated via the Company's website, and any changes to the Company's Privacy Policy is communicated to the data subjects via the posted Privacy policy on the website. (P 1.1-03)	Observed the Company's website to determine that the Company's Privacy Policy was communicated via the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the Privacy Policy revision history and observed the Company's website to determine that any change to the Company's Privacy Policy was communicated to data subjects by the updated policy posted on the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.1-03	The Company has implemented a formal documented Privacy Policy and Privacy Notice which address the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced. (P 1.1-04)	Inspected the Company's Privacy Policy and Privacy Notice to determine that the Company had implemented a formal documented Privacy Policy and Privacy Notice which addressed the following: • The purpose for collecting personal information; • The requirement for implicit or explicit consent to collect, use, and disclose personal information, unless a law or regulation specifically required otherwise and the choices available to individuals; • The choices available to individuals with respect to the collection, use, and disclosure of personal information; • The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, and that personal information is collected only for the purposes identified within the notice and for which explicit approval is given and maintained; • The uses, retention, and disposal of personal information; • How information may be disclosed to third parties; • How individuals may obtain access to their personal information to review, update, and correct; and • How compliance with the Privacy Policy is monitored and enforced. Further, inquired of the CEO to determine that the Privacy Policy which was inspected was in place throughout the specified period.	No exceptions noted.
P 6.2 - The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
P 6.2-01	N/A - dmarcian, Inc. does not disclose to or share personal information with third-parties; therefore, there is no disclosures of personal information requiring authorization. This criterion is not applicable.		

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.3 - The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
P 6.3-01	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved. (CC 7.3-02)	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.4 - The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
P 6.4-01	On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. (CC 1.3-02)	Inspected the most recent vendor risk assessment documentation to determine that management evaluated the third parties that had access to confidential data and/or that performed a managed service related to the operation of the System and determined their risk rating based on their level of access, the sensitivity of the data, and the impact to operations during the specified period. Further, inspected the third party assessment documentation related to a sample of third-parties that had access to confidential data and/or that performed a managed service related to the operation of the System to determine that, based on the risk rating of each selected third party, the Company performed either a vendor security assessment of the third party, reviewed the third party's SOC reports, or the third party was subjected to continuous monitoring. In addition, inspected supporting documentation and inquired of the CEO to determine that there were no issues identified during the selected third-party reviews; however, that if any issues had been identified, each issue would have been researched and corrective actions would have been taken and that this process was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.4-02	The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies . These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments. (CC 1.3-03)	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the CEO to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the third-party contracts related to a sample of new third parties to determine that the Chief Operating Officer reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security, availability, and privacy practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new key vendors and/or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the listing of key vendors and third parties used to pull the listing of new third parties during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no new key vendors and/or third parties during the specified period. Further, inquired of the CEO to determine that there were no new key vendors and/or third parties during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.5 - The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
P 6.5-01	The Company has defined a standard agreement with key vendors and third parties which includes the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies . These commitments contain performance guarantees and address liability for failure to perform, including potential termination of the contract for failure to remediate. The Chief Operating Officer is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security, availability, and privacy practices and commitments. (CC 1.3-03)	Inspected the standard agreement with key vendors and third parties to determine that the Company had defined a standard agreement which included the required security, availability, and privacy commitments in accordance with the Company's security, availability, and privacy policies and that these commitments contained performance guarantees and addressed liability for failure to perform, including potential termination of the contract for failure to remediate. Further, inquired of the CEO to determine that the standard agreement which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the third-party contracts related to a sample of new third parties to determine that the Chief Operating Officer reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security, availability, and privacy practices and commitments.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new key vendors and/or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the listing of key vendors and third parties used to pull the listing of new third parties during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no new key vendors and/or third parties during the specified period. Further, inquired of the CEO to determine that there were no new key vendors and/or third parties during the specified period.	No exceptions noted.
P 6.6 - The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P 6.6-01	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved. (CC 7.3-02)	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.7 - The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
P 6.7-01	When an individual requests his/her personal information, the Company authenticates the individual's identity through a username and password and, upon authentication, provides the information to the individual. (P 5.1-01)	Observed the system configurations related to the personal information request process to determine that the dmarcian System was configured to authenticate an individual's identity through a username and password and that, upon authentication, the dmarcian System was configured to provide the information to the individual. Further, inquired of the Data Protection Officer to determine that these configurations were in place throughout the specified period.	No exceptions noted.
P 6.7-02	If access to personal information is denied, the individual is informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation. (P 5.1-02)	Inspected the tickets and supporting documentation related to a sample of denied information requests to determine that the individual was informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation, for each selected denied information request.	No exceptions noted.
P 6.7-03	Users are able to determine whether the Company maintains personal information about them through an automated system process. Upon authentication, users are provided access to their personal information maintained by the Company. (P 5.1-03)	Observed the automated dmarcian System configurations to determine that users were able to determine whether the Company maintained personal information about them through an automated system process. Further, observed the automated system configurations to determine that, upon authentication, users were provided access to their personal information maintained by the Company. Further, inquired of the CEO to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 6.7-04	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial. (P 5.1-04)	Inspected supporting documentation related to a sample of denied correction of personal information requests to determine that each respective individual was informed, in writing, about the reason his/her request for correction of personal information was denied and how he/she could appeal the denial.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for correction of personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests made by individuals pertaining to the correction of personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for correction of personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for correction of personal information during the specified period.	No exceptions noted.
P 6.7-05	When an individual requests his/her personal information, the Company provides the personal information in an understandable form, at no cost, and within five business days. (P 5.1-05)	Inspected the personal information requests and supporting documentation related to a sample of requests by individuals for their personal information to determine that the Company provided the personal information in an understandable form, at no cost, and within five business days for each selected request.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 6: Privacy Criteria Related to Disclosure and Notification			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of requests for an individual's personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 7: Privacy Criteria Related to Quality			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 7.1 - The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
P 7.1-01	Each request to correct, amend, or append personal information is reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days. (P 5.1-06)	Inspected the log and approvals related to a sample of requests to correct, amend, or append personal information to determine that each selected request was reviewed, authenticated, and processed based on the determination of action (denied or approved) within five business days.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests to correct, amend, or append personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests to correct, amend, or append personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests to correct, amend, or append personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests to correct, amend, or append personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 7: Privacy Criteria Related to Quality			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 7.1-02	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial. (P 5.1-04)	Inspected supporting documentation related to a sample of denied correction of personal information requests to determine that each respective individual was informed, in writing, about the reason his/her request for correction of personal information was denied and how he/she could appeal the denial.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for correction of personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of requests made by individuals pertaining to the correction of personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for correction of personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for correction of personal information during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 8.1 - The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
P 8.1-01	A process is in place to address privacy inquiries, complaints, and/or disputes. Each instance is addressed, and the resolution is documented and communicated to the individual who submitted the privacy inquiry, complaint, and/or dispute.	Inspected the Incident Response Plan and the Privacy Policy to determine that a documented process was in place to address privacy inquiries, complaints, and disputes. Further, inquired of the CEO to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
		Inspected the support tickets related to a sample of privacy inquiries, complaints, and/or disputes to determine that each selected privacy inquiry, complaint, and/or dispute was addressed and that the resolution was documented and communicated to the individual who submitted the privacy inquiry, complaint, and/or dispute.	No exceptions noted.
P 8.1-02	A monitoring solution has been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect potential security threats, including unauthorized access to the network and unauthorized components/devices on the network, and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the Technical Operations Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 8.1-03	When an incident related to system security, availability, and/or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and the corrective actions implemented. (CC 4.2-01)	Inspected the Incident Management Procedure to determine that when an incident related to system security, availability, and/or privacy was detected or reported, a defined incident management process was required to be initiated by appropriate personnel and included a root cause analysis and implemented corrective actions. Further, inquired of the CEO to determine that the Incident Management Procedure which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets, root cause analyses, and supporting documentation related to a sample of security, availability, and/or privacy incidents to determine that a defined incident management process was initiated by appropriate personnel and included a root cause analysis and corrective actions implemented for each selected incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no system security, availability, or privacy incidents detected or reported during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of system security, availability, and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period. Further, inquired of the CEO to determine that there were no system security, availability, or privacy incidents detected or reported during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 8.1-04	Security and privacy incidents are evaluated to determine whether each incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Any issues are researched and resolved. (CC 7.3-02)	Inspected the incident tickets and supporting documentation related to a sample of security and privacy incidents to determine that each selected security or privacy incident was evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information, that the affected information was appropriately identified, and whether there was a failure to comply with applicable laws and regulations. Further, inspected the resolution documentation related to each selected security or privacy incident to determine that each issue was researched and resolved.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no security or privacy incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.
		Inspected the query used to pull the listing of system security and privacy incidents during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no security or privacy incidents during the specified period. Further, inquired of the CEO to determine that there were no security or privacy incidents during the specified period.	No exceptions noted.
P 8.1-05	A formal disciplinary process, up to and including termination, is documented to help ensure the correct and fair treatment of employees who are suspected of non-compliance with the Company's policies and procedures. (CC 1.1-01)	Inspected the Employee Handbook to determine that a formal disciplinary process, up to and including termination, was documented to help ensure the correct and fair treatment of employees who were suspected of non-compliance with the Company's policies and procedures. Further, inquired of the CEO to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 8.1-06	The Company has reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website and intranet. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident. (CC 2.2-02)	Observed the Company's external website and intranet to determine that the Company had reporting mechanisms in place for reporting security, availability, and privacy incidents and compliance concerns, and information to contact the e-mail and phone was communicated to all stakeholders via the Company's external website and intranet. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the incident reports related to a sample of security, availability, and privacy incidents and compliance concerns to determine that each selected incident was reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security, availability, and/or privacy incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the query used to pull the listing of reported security, availability, and privacy incidents and/or compliance concerns during the specified period to determine that the query was accurate to result in a complete population. Inspected the resulting listing to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period. Further, inquired of the CEO to determine that there were no reported security, availability, or privacy incidents and/or compliance concerns during the specified period.	No exceptions noted.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
P 8.1-07	Compliance with objectives related to privacy are reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented. (CC 4.1-01)	Inspected the results from the most recent Privacy Review to determine that compliance with objectives related to privacy were reviewed and documented and that the results of the review were reported to management during the specified period. Further, inspected the results of the review and inquired of the CEO to determine that no problems were identified as a result of the review; however, that if any problems had been identified, a remediation plan would have been developed for each identified problem and that this process was in place throughout the specified period.	No exceptions noted
P 8.1-08	If access to personal information is denied, the individual is informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation. (P 5.1-02)	Inspected the tickets and supporting documentation related to a sample of denied information requests to determine that the individual was informed of the reason, the source of the Company's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such a denial, as specifically permitted or required by law or regulation, for each selected denied information request.	No exceptions noted.
P 8.1-09	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they can appeal the denial. (P 5.1-04)	Inspected supporting documentation related to a sample of denied correction of personal information requests to determine that each respective individual was informed, in writing, about the reason his/her request for correction of personal information was denied and how he/she could appeal the denial.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no requests for correction of personal information during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of the Control Activity.

PRIVACY CATEGORY: Additional Criteria for Privacy			
CRITERIA GROUP 8: Privacy Criteria Related to Monitoring and Enforcement			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the query used to pull the listing of requests made by individuals pertaining to the correction of personal information during the specified period to determine that the listing was accurate to result in a complete population. Inspected the listing to determine that there were no requests for correction of personal information during the specified period. Further, inquired of the Data Protection Officer to determine that there were no requests for correction of personal information during the specified period.	No exceptions noted.
P 8.1-10	The Company's Privacy Policy is communicated via the Company's website, and any changes to the Company's Privacy Policy is communicated to the data subjects via the posted Privacy policy on the website. (P 1.1-03)	Observed the Company's website to determine that the Company's Privacy Policy was communicated via the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected the Privacy Policy revision history and observed the Company's website to determine that any change to the Company's Privacy Policy was communicated to data subjects by the updated policy posted on the Company's website. Further, inquired of the CEO to determine that this process was in place throughout the specified period.	No exceptions noted.