Graphic Village

Graphic Village

Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System

System and Organization Controls (SOC) for Service Organizations Report for the period of October 1, 2022 to March 31, 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 Graphic Village

Scope

We have examined Graphic Village's (the "Company") accompanying description of the Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System (the "System") titled *Graphic Village's Description of its System and Controls* throughout the period October 1, 2022 to March 31, 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 October 1, 2022 to March 31, 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 (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 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 *Graphic Village'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.

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.

FORVIS

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.

Opinion

In our opinion, in all material respects,

A. The description presents Graphic Village's Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System that was designed and implemented throughout the period October 1, 2022 to March 31, 2023, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the period October 1, 2022 to March 31, 2023, to provide reasonable assurance that Graphic Village'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 user entities applied the complementary controls assumed in the design of Graphic Village's controls throughout that period.

C. The controls stated in the description operated effectively throughout the period October 1, 2022 to March 31, 2023, to provide reasonable assurance that Graphic Village's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Graphic Village'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 October 1, 2022 to March 31, 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 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

August 18, 2023

Graphic Village

Section II: Graphic Village's Assertion

We have prepared the accompanying description of Graphic Village's (the "Company") Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System (the "System") titled *Graphic Village's Description of its System and Controls* throughout the period October 1, 2022 to March 31, 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 ("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 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 October 1, 2022 to March 31, 2023, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the period October 1, 2022 to March 31, 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 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 October 1, 2022 to March 31, 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 user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

Section III: Graphic Village's Description of its System and Controls

A. Overview of Services Provided

Scope

The scope of this report includes the Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System performed in the Louisville, KY facility of Graphic Village (the "Company"). In December 2021, Graphic Village announced its acquisition of Mail Louisville, Inc., and the Mail Louisville entity was absorbed into Graphic Village. This report does not include the other offerings provided by Graphic Village.

Services

- Printing of all types including a 7-color digital press and Perfector Presses for longer runs;
- Packaging with Metallic special effects and digital foil capabilities;
- Die Cutting, Fold, Glue, and Tipping;
- Promotional items to build long-lasting brand awareness through personalized products;
- Warehousing, Fulfillment & Kitting with Portal-accessed print-on-demand;
- Mailing Services located within a day's drive of 65 percent of North America's population;
- Connect provides a one-stop gateway for ordering all marketing collateral;
- Creative Services to deliver your eye-catching designs through the most effective channels;
- Brand Development helps you develop a unique brand to improve perceptions;
- Marketing Strategy to engage your target audience and grow your business;
- Graphic Design from digital advertising to package design, web design, and video;
- Custom Content to tell your story through videos, blogs, and social media posts;
- Interactive Marketing array through PURLs, domains, website hosting, social media, and SEO; and
- Election solutions to enhance name recognition and inform your voters.

B. Principal Service Commitments and System Requirements

Graphic Village designs its processes and procedures related to the Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System ("System") to meet its objectives for its print and mail fulfillment services. Those objectives are based on the service commitments that Graphic Village makes to user entities; the laws and regulations that govern the provision of its print and mail fulfillment services; and the financial, operational, and compliance requirements that Graphic Village has established for the services. The print and mail fulfillment services of Graphic Village are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations within the jurisdictions in which Graphic Village operates. Security commitments to user entities are documented and communicated within Service Level Agreements (SLAs) and other customer agreements, as well as within the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role; and

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

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

C. Components of the System Used to Provide the Services

1. Infrastructure

The following indicates Graphic Village's general procedure flow of printing operations:

- Data Transmission - Client transmits files via the Internet;

- Validation -Validation ensures the files are received intact and that the client supplies the required processing instructions;

- Processing - Raw data is composed into pages and made ready for printing and/or electronic presentation;

- Printing - Documents are printed and prepared for inserting;

- Inserting - Documents are folded and enclosed in envelopes and prepared for mailing; and

- Mailing - Documents are delivered to the post office.

The Graphic Village printing operation is an end-to-end system comprising of invoice and statement design and consultation, data transmission, transactional document production, customer service, postal mailing coordination, and quality control.

The infrastructure is housed at Graphic Village's 24,000 S.F. facility located at 12500 Westport Rd, Louisville, KY 40245. Data Specialists manage, cleanse, and certify mail lists using individual networked workstations. The mailing lists are then processed through the National Change of Address (NCOA) to update the mailing in the event the recipient has moved during the past two years. Lastly, multiple networked printers are utilized throughout the system to deliver services.

2. Software

BCC Software, originally Business Computer Center, Inc., is a third-party postal and presort software solution. Data Specialists utilize BCC Software that resides in-house to cleanse and fix addresses provided by clients via incoming file types that include Excel, CSV, XML, TXT, Delimited, etc. The completed address files are then sent to one of the multiple printers via an internal PlanetPress License for spooling to a printer. PlanetPress is also an off-the-shelf software provided by ObjectifLune.

The scope of the report is limited to the BCC and PlanetPress applications.

3. People

The organization is led by the Board of Directors, the Chief Executive Officer, and the Chief Financial Officer. Management and direction for the Company originates from this group based on input from the members of senior management, financial partners, and third-party reviews and assessments. The departmental structure divides operations into multiple divisions, including Finance, Sales, Services, and Technology. Managers and staff within each division are assigned responsibility for the implementation of corporate policies.

4. Data

The types of data provided by customers is dependent upon the services to be provided. For fulfillment services related to advertising or marketing, clients provide public information for Graphic Village to process via the Web, email, hard copy, telephone, or fax. Secure transmission methods are used for clients communicating sensitive information that may include client customers' personally identifiable information (PII). Graphic Village has deployed Secure File Transfer Protocols (SFTP) for the secure transmission of confidential and/or sensitive information over public networks.

5. Policies and Procedures

Procedures are in place to manage the security of customer data. These processes are documented and address the relevant aspects of the security category of the Trust Services Criteria (TSC) within Graphic Village's information technology control environment.

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 Graphic Village is acknowledged by management through the 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;
- Commitment to competence;

- Management's philosophy and operating style; and
- Assignment of authority and responsibility.

Integrity and Ethical Values

A Code of Business Conduct and Ethics is reviewed, updated if applicable, and approved by senior management annually. Personnel are required to read and accept the Code of Business Conduct and Ethics upon their hire and formally reaffirm them annually thereafter. The Code of Business Conduct and Ethics includes a sanctions policy for personnel who violate the documented standards.

Graphic Village has defined and assigned appropriate personnel responsibility for ongoing review and updates to Information Security policies and procedures. Senior management is responsible for oversight of the organization's Information Security practices and standards. Additionally, departmental meetings are held on a periodic basis to monitor and manage the respective department's progress or lack thereof as it relates to their achievement of the department's responsibilities.

The Company has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets. Purchasing authority designations are documented within Graphic Village's corporate bylaws.

Commitment to Competence

Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal (as needed), drug, and employment checks. Before a contractor is onboarded by the Company, the third-party personnel undergo background screening.

Annual performance appraisals are performed with personnel to evaluate performance in their roles with the Company. Gaps in performance are managed through this process to ensure workforce members are held accountable against organizational standards.

Job requirements are documented in the job descriptions, specifying the responsibilities and skills needed for job positions. Job descriptions are reviewed by management on an annual basis for needed changes. Roles and responsibilities are defined in written job-descriptions.

Management's Philosophy and Operating Style

The Louisville, KY operations proceed under direction from senior management who are responsible for maintaining oversight of the organization's control environment.

Assignment of Authority and Responsibility

Reporting relationships and organizational structures are established by senior management as part of organizational planning and adjusted as needed based on changing commitments and requirements. Management has established its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process.

2. Risk Assessment Process

A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and migration strategies for those risks.

As part of the risk management process, Graphic Village annually assesses the potential risks and vulnerabilities of the confidentiality, integrity, and availability of critical or confidential information received or processed internally. An IT risk assessment is conducted on the Louisville, KY Printing and Mailing Facility's Information Technology General Control Environment System, which includes applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Upon completion of an assessment, the execution, development, and implementation of remediation programs is the joint responsibility of the Security Team and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Security Team on the development of a remediation plan.

The annual IT risk assessment is used to identify risks arising from both external and internal sources. The risk assessment process includes the following key steps:

- Scope the assessment;
- Gather information;
- Identify threats;
- Identify vulnerabilities;
- Assess security controls;
- Evaluate the potential impact of findings;
- Determine the level of risk;
- Recommend security controls to mitigate identified risks; and
- Document results.

The Company's Special Meeting Group meets quarterly to discuss strategy and operations, and other factors critical to the business. The Special Meeting Group assesses and responds to security risks identified from vulnerability assessments performed and the annual risk assessment.

Cybersecurity insurance is in place to minimize the financial impact of any loss events.

3. Information and Communication Systems

Graphic Village has implemented policies and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Organizational policies and procedures are reviewed and updated on at least an annual basis. Any changes to the Company's commitments and system requirements are communicated to internal users. Workforce members are granted access to departmental share drives on the Network where applicable policies and procedures are available.

The Company's security commitments are communicated to newly hired employees to enable them to carry out their responsibilities. The Acceptable Use Policy addresses personnel requirements for the proper use of Company assets. The policy reinforces management's commitment to protecting employees, partners, and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. Newly onboarded personnel are required to acknowledge their receipt and understanding of the organization's security commitments. Management has also developed in-house training describing its security commitments and requirements for personnel to support the achievement of objectives.

The Company's Special Meeting Group meets quarterly to communicate information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.

Agreements are established with clients providing sensitive data that include clearly defined terms, conditions, and responsibilities for the Company and clients. Updates or modifications to standard contractual terms and commitments are approved by management prior to contract approval. Contact email addresses and phone numbers are made available on the Company's websites.

4. Monitoring Controls

The information security program establishes relevant control activities through oversight of senior management to ensure risks to the control environment are addressed. An Access Control policy is in place to ensure segregation of duties is enforced and privileges are appropriately assigned to users. The Company's policy and procedure manuals are reviewed annually by senior management.

IT strategic planning sessions are held with key members of management to discuss organizational strategies including IT. A course of action is put in place for any potential risks identified within these working sessions that may affect the organization.

Annual PCI vulnerability scans are performed. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities. Additionally, Graphic Village performs annual risk assessments and communicates results to management for monitoring of corrective actions. Any identified deficiencies are risk rated and evaluated by senior management. The status of deficiencies is monitored until satisfactorily resolved.

E. Control Activities

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 Company who are responsible for the design, development, implementation, and operation of systems affecting system security.

Each employee verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks, prior to his/her start date. The requirements for the completion of background checks on all contracted employees by staffing agencies are outlined within contractual agreements. The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 30 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 and Code of Conduct within 30 days of hire, and annually thereafter.

On a quarterly basis, the Company's Special Meeting Group meets to communicate the information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements. Management reviews the Company's Organizational Chart, 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-related commitments, on its website. The Company has reporting mechanisms in place for reporting security incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident.

3. Risk Assessment

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) 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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved.

On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution.

5. Control Activities

The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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. The General Manager is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate material changes to applicable internal and external users, related parties, and vendors.

6. Logical and Physical Access Controls

Logical Access

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 production databases utilizing Advanced Encryption Standards (AESs). 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 applications, and related databases. Password parameters for the in-scope applications are configured as follows:

- Passwords must be a minimum of eight characters in length,
- Passwords must be changed at least every 90 days,
- Accounts are locked out of the system after five invalid attempts, and
- Password complexity settings are enforced.

Password parameters for the network, network devices, and databases related to the in-scope applications are configured as follows:

- Passwords must be a minimum of eight characters in length,
- Passwords must be changed at least every 90 days,
- Accounts are locked out of the system after five invalid attempts, and
- Password complexity settings are enforced.

The ability to modify data transmission protocols is limited to appropriate users based on job function. Remote access to the network and to the production environment related to the in-scope applications and related databases is restricted to appropriate users via the LogMeIn application. Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function. Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function. Local Administrator access on end-user 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. 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 24 hours of the employee's/contractor's termination date. The Company performs an annual review of access to the network and the in-scope applications to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.

Physical Access

Physical access to the Data Center is reviewed on a quarterly basis by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved. Physical access requests to sensitive areas and the headquarters must be approved by management prior to the granting of access. Terminated employee access to sensitive areas and the headquarters is revoked within 24 hours of termination. The ability to implement changes to physical access rights at sensitive areas and the headquarters is limited to appropriate personnel based on job function to prevent unauthorized changes.

Visitors are required to sign-in at the front desk prior to proceeding into the facility, and all visitors must be escorted to their destination by an authorized employee or their designee. All external access points to sensitive areas and the headquarters are controlled through an electronic badge access system. Badge access is limited to appropriate individuals.

Data Retention

Client information that has exceeded its retention period is purged, destroyed, or overwritten in accordance with the Company's Data Retention and Destruction Policy. Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time, and the Company disposes of sensitive data in accordance with its established retention and destruction standards. Physical assets and paper media that are no longer needed are destroyed by a third-party destruction company.

Network Security

Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment. All transmissions of confidential and/or sensitive electronic information are encrypted as the default setting over public networks via Secure Shell (SSH) File Transfer Protocol (SFTP). Anti-malware software is in place on all workstations and Company-hosted servers related to the in-scope systems. All workstations and Company-hosted servers related to the in-scope systems are updated with current virus definitions to protect data from infection by malicious code or virus.

7. System Operations

A Business Continuity and Disaster Recovery Plan is documented and is tested on an annual basis, and any issues are documented and resolved. Incremental and full backups of the in-scope applications and related databases are configured to be performed in real time and daily, respectively. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.

When an incident related to system security 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.

8. Change Management

The Company has documented a formal Change Control Policy and a formal Patch Management Policy which govern the design, implementation, configuration, modification, and management of the network, the in-scope applications, and their related databases.

Access to promote changes into the production environment is limited to appropriate individuals based on job function. Each change to the network and the in-scope applications must be approved by a member of the Special Meeting Group prior to promotion into the production environment.

Domain server patches are configured to automatically download, and these patches are installed by appropriate personnel on a monthly basis. Build standards are documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. A member of the IT Department completes a configuration checklist for each new server to help ensure that the new server contains the applicable baseline configurations in accordance with the build standard.

9. Risk Management

Cyber insurance is in place to minimize the financial impact of any loss events.

On a quarterly basis, the Company's Special Meeting Group meets to assess and manage risks related to the use of vendors and other third parties that perform a managed service A member of the Legal Department and/or management is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security practices and commitments.

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 Category, Criteria, Graphic Village'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 October 1, 2022 to March 31, 2023 (the "specified period").

H. System Incidents

Management did not identify any significant system incidents during the period October 1, 2022 to March 31, 2023.

I. Complementary User Entity Controls

Graphic Village'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 performing annual user access reviews to Graphic Village's SFTP portal.	CC 6.2*, CC 6.3*
Each user organization is responsible for confirming access to Graphic Village's Louisville, KY Facility services is immediately disabled for terminated user entity personnel.	CC 6.1*, CC 6.2*, CC 6.3*

User Entity Controls	Related Criteria
Each user organization is responsible for changing passwords to Graphic Village's SFTP portal periodically – at least every 90 days.	CC 6.1*
Each user organization is responsible for deleting its personal data from Graphic Village resources when necessary.	CC 6.5*
Each user organization is responsible for notifying Graphic Village of any issues, problems, or needed changes.	CC 2.2*, CC 2.3*, CC 7.3*, CC 7.4*, CC 8.1*

* 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 Category, Criteria, Graphic Village'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, 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. 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 Category, 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.

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 Trust Services Category			
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	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security.	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.
CC 1.1-02	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.	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 General Manager to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.1-03	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.
CC 1.1-04	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.1-05	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 30 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 policies and procedures to employees and contractors. Further, inquired of the General Manager to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		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 30 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.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as the annual security awareness training was last completed in June, 2022 and was not scheduled to be completed next until June, 2023, which is outside of the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the most recent Security Awareness Acknowledgments related to a sample of employees and contractors to determine that annual security awareness training was last completed in June, 2022, which was outside of the specified period. Further, inquired of the General Manager to determine that Security Awareness Training is completed on an annual basis and that the next training was scheduled to be completed in June, 2023, which is outside of the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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 and Code of Conduct within 30 days of hire, and annually thereafter.	Inspected the Employee Handbook and Code of Conduct 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 and Code of Conduct within 30 days of hire.	No exceptions noted.
		Inspected the Employee Handbook and Code of Conduct and Policy Acknowledgement Forms related to a sample of active employees and contractors to determine that each selected active 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 and Code of Conduct during the specified period.	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 a quarterly basis, the Company's Special Meeting Group meets to communicate the information needed to fulfill their roles with respect to the achievement of the Company's service commitments and systems requirements.	Inspected the meeting minutes related to a sample of quarters to determine that the Company's Special Meeting Group met during the selected quarter to communicate the 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 Chart, 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 General Manager 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 Trust Services Category			
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 General Manager 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 - 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	The General Manager is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate material changes to applicable internal and external users, related parties, and vendors.	Observed the security 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 General Manager 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 policies to determine that the General Manager was responsible for changes to security 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 Trust Services Category			
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 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 revisions made to the security policies during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of revisions made to the security policies during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no revisions made to the security policies during the specified period. Further, inquired of the General Manager to determine that there were no revisions made to the security policies during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.3-02	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.3-03	A member of the Legal Department and/or management is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security practices and commitments.	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department and/or management reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no new vendors or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this Control Activity.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of new vendors and third parties during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new vendors or third parties during the specified period. Further, inquired of the General Manager to determine that there were no new vendors or third parties during the specified period.	No exceptions noted.
CC 1.3-04	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.
CC 1.3-05	Management reviews the Company's Organizational Chart, 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 General Manager 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 General Manager 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 Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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 employee verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks, prior to his/her start date.	Inspected the background checks and supporting documentation related to a sample of new employees to determine that each selected new employee was verified against regulatory screening databases, including at a minimum, criminal (as needed) and drug checks, prior to his/her start date.	No exceptions noted.
CC 1.4-02	The requirements for the completion of background checks on all contracted employees by staffing agencies are outlined within contractual agreements.	Inspected the contracts related to a sample of staffing agencies used by the Company to determine that the requirements for the completion of background checks on all contracted employees by staffing agencies are outlined within the contractual agreement with each selected staffing agency.	No exceptions noted.
CC 1.4-03	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.
CC 1.4-04	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 1.1-02)	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 General Manager to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 1.4-05	Performance reviews are performed on an annual basis to help ensure that each employee's skill set matches his/her job responsibilities. (CC 1.1-03)	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 1.4-06	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 1.4-07	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 30 days of his/her start date, and annually thereafter. (CC 1.1-05)	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security policies and procedures to employees and contractors. Further, inquired of the General Manager to determine that the security awareness program training materials which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		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 30 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.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as the annual security awareness training was last completed in June, 2022 and was not scheduled to be completed next until June, 2023, which is outside of the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the most recent Security Awareness Acknowledgments related to a sample of employees and contractors to determine that annual security awareness training was last completed in June, 2022, which was outside of the specified period. Further, inquired of the General Manager to determine that Security Awareness Training is completed on an annual basis and that the next training was scheduled to be completed in June, 2023, which is outside of the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 1: Common Criteria Related to Control Environment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	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 1.1-02)	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 General Manager 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 Chart, 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 General Manager 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 Trust Services Category			
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 General Manager 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 1.1-03)	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 Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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 Trust Services Category			
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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met.	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved.	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.1-03	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 2.1-04	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution.	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability 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 Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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) 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) 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 2.1-06	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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-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-related commitments. Further, inquired of the General Manager to determine that a description of the in-scope applications and related databases and its 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 incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident.	Observed the Company's external website to determine that information to contact the Company via e-mail and phone was communicated to all stakeholders via the Company's external website. Further, inquired of the General Manager 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 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 incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no security incidents, compliance concerns, or suspected ethics/policy violations 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 Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of security incidents, compliance concerns, or suspected ethics/policy violations during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Further, inquired of the General Manager to determine that there were no security incidents, compliance concerns, and suspected ethics/policy violations during the specified period.	No exceptions noted.
CC 2.2-03	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.
CC 2.2-04	The General Manager is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate material changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security 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 General Manager to determine that these practices and commitments were available on the Company's intranet and website throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the security policies to determine that the General Manager was responsible for changes to security 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 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 revisions made to the security policies during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of revisions made to the security policies during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no revisions made to the security policies during the specified period. Further, inquired of the General Manager to determine that there were no revisions made to the security policies during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 2.2-05	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 2.2-06	The Company has implemented a security awareness program to communicate the information security policies and procedures to new employees and contractors. Each new employee and contractor is required to complete the training program within 30 days of his/her start date, and annually thereafter. (CC 1.1-05)	Inspected the security awareness program training materials to determine that the Company had implemented a security awareness program to communicate the security policies and procedures to employees and contractors. Further, inquired of the General Manager 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 30 days of his/her start date.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		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.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as the annual security awareness training was last completed in June, 2022 and was not scheduled to be completed next until June, 2023, which is outside of the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the most recent Security Awareness Acknowledgments related to a sample of employees and contractors to determine that annual security awareness training was last completed in June, 2022, which was outside of the specified period. Further, inquired of the General Manager to determine that Security Awareness Training is completed on an annual basis and that the next training was scheduled to be completed in June, 2023, which is outside of the specified period.	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 and Code of Conduct within 30 days of hire, and annually thereafter. (CC 1.1-06)	Inspected the Employee Handbook and Code of Conduct 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 and Code of Conduct within 30 days of hire.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the Employee Handbook and Code of Conduct and Policy Acknowledgement Forms related to a sample of active employees and contractors to determine that each selected active 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 and Code of Conduct during the specified period.	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	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-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-related commitments. Further, inquired of the General Manager to determine that a description of the in-scope applications and related databases and its services was on the Company's website throughout the specified period.	No exceptions noted.
CC 2.3-02	The General Manager is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate material changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security 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 General Manager 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 policies to determine that the General Manager was responsible for changes to security 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 Trust Services Category			
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 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 revisions made to the security policies during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of revisions made to the security policies during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no revisions made to the security policies during the specified period. Further, inquired of the General Manager to determine that there were no revisions made to the security policies during the specified period.	No exceptions noted.
CC 2.3-03	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's external website to determine that information to contact the Company via e-mail and phone was communicated to all stakeholders via the Company's external website. Further, inquired of the General Manager to determine that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 2: Common Criteria Related to Communication and Information			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident reports related to a sample of security 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 incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents, compliance concerns, or suspected ethics/policy violations during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Further, inquired of the General Manager to determine that there were no security incidents, compliance concerns, and suspected ethics/policy violations during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.
CC 3.1-02	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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 Trust Services Category			
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) 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) 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) 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) 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 Trust Services Category			
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 3.2-02	A member of the Legal Department and/or management is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security practices and commitments. (CC 1.3-03)	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department and/or management reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no new vendors or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this Control Activity.
		Inspected the parameters used to pull the listing of new vendors and third parties during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new vendors or third parties during the specified period. Further, inquired of the General Manager to determine that there were no new vendors or third parties during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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) 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) 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 Chart, 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 General Manager 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 General Manager 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 Trust Services Category			
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 Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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) 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) 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 Trust Services Category			
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	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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.1-03	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved 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 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 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 security incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents 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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 4.2-03	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 4.2-04	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 4.2-05	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 1.1-02)	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 General Manager to determine that the Employee Handbook which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1-03	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 5.1-04	Management reviews the Company's Organizational Chart, 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 General Manager 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 General Manager 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 Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.1-05	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager to determine that the policies which were inspected were in place throughout the specified period.	No exceptions noted.
CC 5.1-06	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) 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) 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 Trust Services Category			
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	Access to promote changes into the production environment is limited to appropriate individuals based on job function.	Inspected the listing of users with access to promote changes into the production environment 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 5.2-02	Each change to the network and the in-scope applications must be approved by a member of the Special Meeting Group prior to promotion into the production environment.	Inspected the change tickets and supporting documentation related to a sample of changes to the network and the in-scope applications to determine that each selected change was approved by a member of the Special Meeting Group prior to promotion into the production environment.	No exceptions noted.
CC 5.2-03	The Company has documented a formal Change Control Policy and a formal Patch Management Policy which govern the design, implementation, configuration, modification, and management of the network, the in-scope applications, and their related databases.	Inspected the Change Control Policy and the Patch Management Policy to determine that the Company had documented a formal Change Control Policy and a formal Patch Management Policy which governed the design, implementation, configuration, modification, and management of the network, the in-scope applications, and their related databases. Further, inquired of the General Manager to determine that the Change Control Policy and the Patch Management Policy which were inspected were in place throughout the specified period.	No exceptions noted.
CC 5.2-04	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function.	Inspected the listing of users with Administrative access to the in-scope applications 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 5.2-05	Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function.	Inspected the listing of users with Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion prevention devices, and SFTP servers 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 5.2-06	Local Administrator access on end user devices is restricted to appropriate individuals based on job function.	Inspected the listing of users with Local Administrator access on end user devices 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.
CC 5.2-07	Valid user IDs and passwords are required to access the Company's network, in-scope applications, and related databases.	Observed the authentication configurations for the network, the in-scope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, the in-scope applications, and the related databases. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 5.2-08	Domain server patches are configured to automatically download, and these patches are installed by appropriate personnel on a monthly basis.	Observed the patching configurations to determine that domain server patches were configured to automatically download patches. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the patch documentation related to a sample of months to determine that domain server patches were installed for each selected month.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the listing of users with the ability to install domain server patches 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 General Manager to determine that each user on the listing 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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts 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 Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 5.3-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system 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 Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.
CC 5.3-03	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 5.3-04	When an incident related to system security 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control 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 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 security incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents during the specified period.	No exceptions noted.
CC 5.3-05	The Company has written job descriptions specifying the responsibilities of and professional requirements for job positions within the Company who are responsible for the design, development, implementation, and operation of systems affecting system security. (CC 1.1-01)	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 to determine that the Company had written job descriptions specifying the responsibilities of and professional requirements for each selected job positions within the Company who were responsible for the design, development, implementation, and operation of systems affecting system security.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 1.1-03)	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	The General Manager is responsible for changes to security practices and commitments. A formal process is documented and is followed to communicate material changes to applicable internal and external users, related parties, and vendors. (CC 1.3-01)	Observed the security 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 General Manager 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 policies to determine that the General Manager was responsible for changes to security 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 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 revisions made to the security policies 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 Trust Services Category			
CRITERIA GROUP 5: Common Criteria Related to Control Activities			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of revisions made to the security policies during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no revisions made to the security policies during the specified period. Further, inquired of the General Manager to determine that there were no revisions made to the security policies during the specified period.	No exceptions noted.
CC 5.3-08	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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 Trust Services Category			
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	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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-02	The backup tool is configured to automatically protect backups of the in-scope production 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 production databases with Advanced Encryption Standards (AESs). Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-03	Valid user IDs and passwords are required to access the Company's network, in-scope applications, and related databases. (CC 5.2-07)	Observed the authentication configurations for the network, the in-scope applications, and the related databases to determine that a valid user ID and password were required to access the Company's network, the in-scope applications, and the related databases. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-04	Build standards are documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. A member of the IT Department completes a configuration checklist for each new server to help ensure that the new server contains the applicable baseline configurations in accordance with the build standard.	Inspected the Server Build Standards to determine that build standards were documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. Further, inquired of the General Manager to determine that the Server Build Standards which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 Build Configuration Checklists related to a sample of new servers to determine that a member of the IT Department completed a configuration checklist for each selected new server supporting the in-scope systems to help ensure that each selected new server contained the applicable baseline configurations in accordance with the build standard.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new servers during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the population of new servers during the period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new servers during the specified period. Further, inquired of the General Manager to determine that there were no new servers during the specified period.	No exceptions noted.
CC 6.1-05	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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.
CC 6.1-06	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 24 hours 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 24 hours of the employee's/contractor's termination date.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-07	Password parameters for the in-scope applications are configured as follows: • Passwords must be a minimum of eight characters in length, • Passwords must be changed at least every 90 days, • Accounts are locked out of the system after five invalid attempts, and • Password complexity settings are enforced.	Observed the password configurations that governed user access to the in-scope applications to determine that password parameters for the in-scope applications were configured as follows: • Passwords must be a minimum of eight characters in length, • Passwords must be changed at least every 90 days, • Accounts are locked out of the system after five invalid attempts, and • Password complexity settings are enforced. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-08	Password parameters for the network, network devices, and databases related to the in-scope applications are configured as follows: • Passwords must be a minimum of eight characters in length, • Passwords must be changed at least every 90 days, • Accounts are locked out of the system after five invalid attempts, and • Password complexity settings are enforced.	Observed the password configurations that governed user access to the network, network devices, and databases related to the in-scope applications to determine that password parameters for the network, network devices, operating systems, and databases related to the in-scope applications were configured as follows: • Passwords must be a minimum of eight characters in length, • Passwords must be changed at least every 90 days, • Accounts are locked out of the system after five invalid attempts, and • Password complexity settings are enforced. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.1-09	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 General Manager 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 Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-10	Remote access to the network and to the production environment related to the in-scope applications and related databases is restricted to appropriate users via the LogMeIn application.	Observed the remote access authentication configurations to determine that remote access to the network and to the production environment related to the in-scope applications and related databases was restricted via the LogMeIn application. Further, inquired of the General 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 the network and to the production environment related to the in-scope applications and related databases 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.1-11	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-04)	Inspected the listing of users with Administrative access to the in-scope applications 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.
CC 6.1-12	Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion prevention devices, and SFTP servers 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 General Manager 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 Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.1-13	Local Administrator access on end user devices is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listing of users with Local Administrator access on end user devices 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception 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 management 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 management prior to access being modified.	No exceptions noted.
CC 6.2-02	The Company performs an annual review of access to the network and the in-scope applications to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved.	Inspected the access review documentation to determine that the Company performed a review of access to the network, the in-scope applications, and their related databases during the specified period to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the General Manager to determine that no issues were identified as a result of the selected review; 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 Trust Services Category			
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 24 hours of the employee's/contractor's termination date. (CC 6.1-06)	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 24 hours 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	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 24 hours of the employee's/contractor's termination date. (CC 6.1-06)	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 24 hours of the employee's/contractor's termination date.	No exceptions noted.
CC 6.3-02	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 management 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 management prior to access being modified.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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	The Company performs an annual review of access to the network and the in-scope applications to help ensure that user access is appropriate. Any issues identified as a result of these reviews are communicated and resolved. (CC 6.2-02)	Inspected the access review documentation to determine that the Company performed a review of access to the network, the in-scope applications, and their related databases during the specified period to help ensure that user access was appropriate. Further, inspected supporting review documentation and inquired of the General Manager to determine that no issues were identified as a result of the selected review; 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	Physical access to the Data Center is reviewed on a quarterly basis by management to validate that employee access is commensurate with job responsibilities. Any issues identified are researched and resolved.	Inspected the physical access review documentation related to a sample of quarters to determine that physical access to the Data Center was reviewed by management during each selected quarter to validate that employee access was commensurate with job responsibilities. Further, inspected supporting documentation and inquired of the General Manager 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 6.4-02	Physical access requests to sensitive areas and the headquarters must be approved by management prior to the granting of access.	Inspected the physical access requests and approvals related to a sample of individuals granted new access to sensitive areas and locations to determine that each selected individual's access was approved by management prior to the granting of access.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.4-03	Terminated employee access to sensitive areas and the headquarters is revoked within 24 hours of termination.	Inspected the access removal tickets and supporting documentation related to a sample of terminated employees to determine that each selected employee's access to sensitive areas and locations was revoked within 24 hours of termination.	No exceptions noted.
CC 6.4-04	The ability to implement changes to physical access rights at sensitive areas and the headquarters is limited to appropriate personnel based on job function to prevent unauthorized changes.	Inspected the listing of users with the ability to implement changes to physical access rights at sensitive areas and locations 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 to prevent unauthorized changes. Further, inquired of the General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.
CC 6.4-05	Visitors are required to sign-in at the front desk prior to proceeding into the facility, and all visitors must be escorted to their destination by an authorized employee or their designee.	Observed the visitor process to determine that visitors were required to sign-in at the front desk prior to proceeding into the facility, and all visitors were escorted to their destination by an authorized employee or their designee. Further inquired of the General Manager to determine that this process was in place throughout the specified period.	No exceptions noted.
		Inspected Visitor Log for a sample of business days to determine that visitor/temporary access to sensitive areas and locations was logged on each selected business day.	No exception noted.
CC 6.4-06	All external access points to sensitive areas and the headquarters are controlled through an electronic badge access system. Badge access is limited to appropriate individuals.	Observed all external access points to sensitive areas and locations to determine that all external access points to sensitive areas and locations were controlled through an electronic badge access system. Further, inquired of the General Manager to determine that this process was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 listing of individuals with access to sensitive areas and locations and the corresponding job titles for a sample of those individuals to determine that each selected individual was appropriate to have this access based on job function. Further, inquired of the General Manager to determine that each selected individual was appropriate to have this access.	No exception noted.
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	Client information which has exceeded its retention period is purged, destroyed, or overwritten in accordance with the Company's Data Retention and Destruction Policy.	Inspected the Company's Data Retention and Destruction Policy to determine that the policy 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 General Manager to determine that the Data Retention and Destruction Policy which was inspected was in place throughout the specified period.	No exceptions noted.
CC 6.5-02	Physical assets and paper media that are no longer needed are destroyed by a third-party destruction company.	Inspected the certificates of destruction and supporting documentation related to a sample of physical assets and paper media that were no longer needed to determine that each selected sample was destroyed by a third-party destruction company.	No exceptions noted.
CC 6.5-03	Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time, and the Company disposes of sensitive data in accordance with its established retention and destruction standards.	Inspected the Data Retention and Destruction Policy 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 the Company disposed of sensitive data in accordance with its established retention and destruction standards. Further, inquired of the General Manager to determine that the Data Retention and Destruction Policy which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 - 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts 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 Trust Services Category			
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 parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 6.6-03	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system 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 Trust Services Category			
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 parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during 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 6.1-01)	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 General Manager 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 the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion prevention devices, and SFTP servers 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.6-06	Local Administrator access on end user devices is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listing of users with Local Administrator access on end user devices 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.6-07	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 24 hours of the employee's/contractor's termination date. (CC 6.1-06)	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 24 hours of the employee's/contractor's termination date.	No exceptions noted.
CC 6.6-08	The ability to modify data transmission protocols is limited to appropriate users based on job function. (CC 6.1-09)	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 General Manager 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 Secure Shell (SSH) File Transfer Protocol (SFTP).	Observed the transmission configurations to determine that all transmissions of confidential and/or sensitive electronic information were encrypted as the default setting over public networks via Secure Shell (SSH) File Transfer Protocol (SFTP). Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.7-02	Access to the backup tool is restricted to appropriate individuals based on job function. (CC 6.1-01)	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 General Manager 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 Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.7-03	The backup tool is configured to automatically protect backups of the in-scope production databases utilizing Advanced Encryption Standards (AESs). (CC 6.1-02)	Observed the backup tool configurations to determine that the backup tool was configured to automatically protect backups of the in-scope production databases with Advanced Encryption Standards (AESs). Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.7-06	Direct access to the in-scope databases is restricted to appropriate users based on job function. (CC 6.1-05)	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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.
CC 6.7-07	Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion prevention devices, and SFTP servers 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.7-08	Local Administrator access on end user devices is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listing of users with Local Administrator access on end user devices 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.7-09	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 24 hours of the employee's/contractor's termination date. (CC 6.1-06)	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 24 hours of the employee's/contractor's termination date.	No exceptions noted.
CC 6.7-10	Remote access to the network and to the production environment related to the in-scope applications and related databases is restricted to appropriate users via the LogMeIn application. (CC 6.1-10)	Observed the remote access authentication configurations to determine that remote access to the network and to the production environment related to the in-scope applications and related databases was restricted via the LogMeIn application. Further, inquired of the General 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 the network and to the production environment related to the in-scope applications and related databases 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 General Manager 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	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 24 hours of the employee's/contractor's termination date. (CC 6.1-06)	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 24 hours of the employee's/contractor's termination date.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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	Anti-malware software is in place on all workstations and Company-hosted servers related to the in-scope systems. All workstations and Company-hosted servers related to the in-scope systems are updated with current virus definitions to protect data from infection by malicious code or virus.	Observed the anti-malware software global configurations to determine that anti-malware software was in place on all workstations and Company-hosted servers related to the in-scope systems, and that the software was configured to update with current virus definitions to protect data from infection by malicious code or virus. Further, inquired of General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
CC 6.8-03	Access to promote changes into the production environment is limited to appropriate individuals based on job function. (CC 5.2-01)	Inspected the listing of users with access to promote changes into the production environment 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.8-04	Build standards are documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. A member of the IT Department completes a configuration checklist for each new server to help ensure that the new server contains the applicable baseline configurations in accordance with the build standard. (CC 6.1-04)	Inspected the Server Build Standards to determine that build standards were documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. Further, inquired of the General Manager to determine that the Server Build Standards which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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 Build Configuration Checklists related to a sample of new servers to determine that a member of the IT Department completed a configuration checklist for each selected new server supporting the in-scope systems to help ensure that each selected new server contained the applicable baseline configurations in accordance with the build standard.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new servers during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the population of new servers during the period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new servers during the specified period. Further, inquired of the General Manager to determine that there were no new servers during the specified period.	No exceptions noted.
CC 6.8-05	Administrative access to the in-scope applications and related databases is restricted to appropriate individuals based on job function. (CC 5.2-04)	Inspected the listing of users with Administrative access to the in-scope applications 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 6.8-06	Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion detection devices, and SFTP servers is restricted to appropriate individuals based on job function. (CC 5.2-05)	Inspected the listing of users with Administrative access to the network and the in-scope utilities, including access to firewalls, intrusion prevention devices, and SFTP servers 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 6.8-07	Local Administrator access on end user devices is restricted to appropriate individuals based on job function. (CC 5.2-06)	Inspected the listing of users with Local Administrator access on end user devices 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exception noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.1-02	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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 7.1-03	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
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	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.2-02	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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 7.2-03	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.
CC 7.2-04	When an incident related to system security 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
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 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 security incidents during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents during 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	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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 7.3-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-03	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.3-04	When an incident related to system security 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy 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 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 security 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents during the specified period.	No exceptions noted.
CC 7.3-05	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-06	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's external website to determine that information to contact the Company via e-mail and phone was communicated to all stakeholders via the Company's external website. Further, inquired of the General Manager 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 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 incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents, compliance concerns, or suspected ethics/policy violations during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Further, inquired of the General Manager to determine that there were no security incidents, compliance concerns, and suspected ethics/policy violations during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.3-07	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) 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) 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	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. Alert notifications are generated, logged, tracked, reported, and resolved when specific predefined conditions are met. (CC 2.1-01)	Observed the IDS configurations to determine that the IDS was 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 General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the escalation procedures and the support tickets related to a sample of alert notifications to determine that each selected alert notification was logged, tracked, reported, and resolved.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no IDS alerts during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the system-generated listing of IDS alerts during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no IDS alerts during the specified period. Further, inquired of the General Manager to determine that there were no IDS alerts during the specified period.	No exceptions noted.
CC 7.4-02	A monitoring solution has been implemented to detect unauthorized access to the network. Alerts are automatically sent to members of the Security Team based upon predefined events, and any identified risks are logged within a ticketing system and are investigated and resolved. (CC 2.1-02)	Observed the monitoring system configurations to determine that a monitoring solution had been implemented to detect unauthorized access to the network and that alerts were automatically sent to members of the Security Team based upon predefined events. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incident tickets and supporting documentation related to a sample of risks identified by the monitoring solution to determine that each selected risk was logged within a ticketing system and was investigated 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 risks identified by the monitoring system during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of actionable risks identified by the monitoring system during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no actionable risks identified by the monitoring system during the specified period. Further, inquired of the General Manager to determine that there were no actionable risks identified by the monitoring system during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-03	On a quarterly basis, PCI vulnerability scans are performed by a third party for all internet-facing infrastructure to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system until resolution. (CC 2.1-04)	Inspected the PCI vulnerability scanning reports related to a sample of quarters to determine that PCI vulnerability scans were performed by a third party for all internet-facing infrastructure during each selected quarter to detect new and unknown vulnerabilities. Further, inspected the scan results and inquired of the General Manager to determine that no critical/high vulnerabilities were identified during the selected scans; however, that if any critical/high vulnerabilities had been identified, each critical/high vulnerability would have been researched and resolved and that this process was in place throughout the specified period.	No exceptions noted.
CC 7.4-04	When an incident related to system security 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy 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 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 security 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents during the specified period.	No exceptions noted.
CC 7.4-05	The Company has implemented a formal written Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy which collectively address the security 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 1.1-04)	Observed the Company's intranet to determine that the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy were posted on the Company's intranet. Further, inquired of the General Manager to determine that these policies were in place and were available on the intranet throughout the specified period.	No exceptions noted.
		Inspected the Security Policy, Incident Response Policy, Access Control Policy, Password Policy, Workstation Security Policy, and Data Retention Policy to determine that these policies collectively addressed the security 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 General Manager 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-06	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's external website to determine that information to contact the Company via e-mail and phone was communicated to all stakeholders via the Company's external website. Further, inquired of the General Manager 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 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 incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the listing of security incidents, compliance concerns, or suspected ethics/policy violations during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Further, inquired of the General Manager to determine that there were no security incidents, compliance concerns, and suspected ethics/policy violations during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 7.4-07	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) 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) 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 to determine that a Business Continuity and Disaster Recovery Plan was documented. Further, inquired of the General Manager to determine that the Business Continuity and Disaster Recovery Plan which was inspected was in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the most recent testing results to determine that the Business Continuity and Disaster Recovery Plan was tested during the specified period. Further, inspected the test results and inquired of the General Manager 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.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as the Business Continuity and Disaster Recovery Plan was last tested in July, 2022 and was not scheduled to be completed next until July, 2023, which is outside of the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the most recent BCDRP testing results to determine the Business Continuity and Disaster Recovery Plan was last tested in July, 2022, which was outside of the specified period. Further, inquired of the General Manager to determine that the BCDRP test is completed on an annual basis and that the next test was scheduled to be completed in July, 2023, which is outside of the specified period.	No exceptions noted.
CC 7.5-02	Incremental and full backups of the in-scope applications and related databases are configured to be performed in real time and daily, respectively. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved.	Observed the incremental backup configurations for the in-scope applications and related databases to determine that incremental and full backups of the in-scope applications and related databases were configured to be performed real time and daily, respectively, and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the incremental backups related to a sample of days to determine that incremental backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted.
		Inspected the full backups related to a sample of days to determine that full backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted.
CC 7.5-03	When an incident related to system security 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 Response Policy to determine that when an incident related to system security 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 General Manager to determine that the Incident Response Policy 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 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 security 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of security incidents during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents during the specified period. Further, inquired of the General Manager to determine that there were no security incidents during the specified period.	No exceptions noted.
CC 7.5-04	The Company has reporting mechanisms in place for reporting security incidents and compliance concerns through e-mail and phone. These mechanisms are communicated to all stakeholders via the Company's external website. Each report is reviewed by appropriate management personnel, based on the nature of the suspected ethics/policy violation claim or suspected security incident. (CC 2.2-02)	Observed the Company's external website to determine that information to contact the Company via e-mail and phone was communicated to all stakeholders via the Company's external website. Further, inquired of the General Manager 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 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 incident.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no security incidents, compliance concerns, or suspected ethics/policy violations 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 Trust Services Category			
CRITERIA GROUP 7: Common Criteria Related to Systems Operations			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the parameters used to pull the listing of security incidents, compliance concerns, or suspected ethics/policy violations during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no security incidents, compliance concerns, or suspected ethics/policy violations during the specified period. Further, inquired of the General Manager to determine that there were no security incidents, compliance concerns, and suspected ethics/policy violations during the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
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	Access to promote changes into the production environment is limited to appropriate individuals based on job function. (CC 5.2-01)	Inspected the listing of users with access to promote changes into the production environment 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 General Manager to determine that each user on the listing was appropriate to have this access.	No exceptions noted.
CC 8.1-02	Each change to the network and the in-scope applications must be approved by a member of the Special Meeting Group prior to promotion into the production environment. (CC 5.2-02)	Inspected the change tickets and supporting documentation related to a sample of changes to the network and the in-scope applications to determine that each selected change was approved by a member of the Special Meeting Group prior to promotion into the production environment.	No exceptions noted.
CC 8.1-03	The Company has documented a formal Change Control Policy and a formal Patch Management Policy which govern the design, implementation, configuration, modification, and management of the network, the in-scope applications, and their related databases. (CC 5.2-03)	Inspected the Change Control Policy and the Patch Management Policy to determine that the Company had documented a formal Change Control Policy and a formal Patch Management Policy which governed the design, implementation, configuration, modification, and management of the network, the in-scope applications, and their related databases. Further, inquired of the General Manager to determine that the Change Control Policy and the Patch Management Policy which were inspected were in place throughout the specified period.	No exceptions noted.
CC 8.1-05	Build standards are documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. A member of the IT Department completes a configuration checklist for each new server to help ensure that the new server contains the applicable baseline configurations in	Inspected the Server Build Standards to determine that build standards were documented to provide consistency when building, implementing, and upgrading servers supporting the in-scope systems. Further, inquired of the General Manager to determine that the Server Build Standards which were inspected were in place throughout the specified period.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
	accordance with the build standard. (CC 6.1-04)	Inspected the Build Configuration Checklists related to a sample of new servers to determine that a member of the IT Department completed a configuration checklist for each selected new server supporting the in-scope systems to help ensure that each selected new server contained the applicable baseline configurations in accordance with the build standard.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as there were no new servers during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this portion of the Control Activity.
		Inspected the parameters used to pull the population of new servers during the period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new servers during the specified period. Further, inquired of the General Manager to determine that there were no new servers during the specified period.	No exceptions noted.
CC 8.1-06	Domain server patches are configured to automatically download, and these patches are installed by appropriate personnel on a monthly basis. (CC 5.2-08)	Observed the patching configurations to determine that domain server patches were configured to automatically download patches. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the patch documentation related to a sample of months to determine that domain server patches were installed for each selected month.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 8: Common Criteria Related to Change Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the listing of users with the ability to install domain server patches 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 General Manager 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 Trust Services Category			
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	Cyber insurance is in place to minimize the financial impact of any loss events.	Inspected the cyber insurance policy to determine that cyber insurance was in place to minimize the financial impact of any loss events. Further, inquired of the General Manager to determine that the cyber 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 to determine that a Business Continuity and Disaster Recovery Plan was documented. Further, inquired of the General Manager to determine that the Business Continuity and Disaster Recovery Plan which was inspected was in place throughout the specified period.	No exceptions noted.
		Inspected the most recent testing results to determine that the Business Continuity and Disaster Recovery Plan was tested during the specified period. Further, inspected the test results and inquired of the General Manager 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.	The Service Auditor noted that this portion of the Control Activity did not operate during the specified period, as the Business Continuity and Disaster Recovery Plan was last tested in July, 2022 and was not scheduled to be completed next until July, 2023, which is outside of 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 Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
		Inspected the most recent BCDRP testing results to determine the Business Continuity and Disaster Recovery Plan was last tested in July, 2022, which was outside of the specified period. Further, inquired of the General Manager to determine that the BCDRP test is completed on an annual basis and that the next test was scheduled to be completed in July, 2023, which is outside of the specified period.	No exceptions noted.
CC 9.1-03	Incremental and full backups of the in-scope applications and related databases are configured to be performed in real time and daily, respectively. The backup system is configured to alert IT personnel of any backup failures, and any repeated backup failures are investigated and resolved. (CC 7.5-02)	Observed the incremental backup configurations for the in-scope applications and related databases to determine that incremental and full backups of the in-scope applications and related databases were configured to be performed real time and daily, respectively, and that the backup system was configured to alert IT personnel of any backup failures. Further, inquired of the General Manager to determine that these configurations were in place throughout the specified period.	No exceptions noted.
		Inspected the incremental backups related to a sample of days to determine that incremental backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted.
		Inspected the full backups related to a sample of days to determine that full backups of the in-scope applications and related databases were completed for each selected day, or if the backups failed repeatedly on the selected day, an alert was sent to IT personnel and the backup failure was investigated and resolved.	No exceptions noted.

COMMON CRITERIA CATEGORY: Criteria Common to the Security Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.1-04	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) 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) 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 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) 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) 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 Trust Services Category			
CRITERIA GROUP 9: Common Criteria Related to Risk Management			
Control Activity Description		**Tests Performed by Service Auditor**	**Results of Testing**
CC 9.2-02	A member of the Legal Department and/or management is responsible for reviewing and approving of all new third-party contracts to help ensure that they include the applicable security practices and commitments. (CC 1.3-03)	Inspected the third-party contracts related to a sample of new third parties to determine that a member of the Legal Department and/or management reviewed and approved each selected new third-party contract to help ensure that each agreement included the applicable security practices and commitments.	The Service Auditor noted that this Control Activity did not operate during the specified period, as there were no new vendors or third parties during the specified period. Therefore, the Service Auditor could not test the operating effectiveness of this Control Activity.
		Inspected the parameters used to pull the listing of new vendors and third parties during the specified period to determine that the parameters were accurate to result in a complete population. Inspected the resulting listing to determine that there were no new vendors or third parties during the specified period. Further, inquired of the General Manager to determine that there were no new vendors or third parties during the specified period.	No exceptions noted.
CC 9.2-03	On a quarterly basis, the Company's Special Meeting Group meets to assess and manage risks related to the use of vendors and other third parties that perform a managed service.	Inspected the meeting minutes related to a sample of quarters to determine that the Company's Special Meeting Group met during the selected quarter to assess and manage risks related to the use of vendors and other third parties that perform a managed service.	No exceptions noted.