Report on Controls at a Service Organization Relevant to Security and Availability and Tests of Operating Effectiveness

November 16, 2016 through November 15, 2017

SOC 2 Type 2

AT 101

TABLE OF CONTENTS

SECTION I – INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Zane Alsabery
CEO
Alchemy
1200 West 7th Street, Suite L1-100
Los Angeles, CA 90017

Scope

We have examined Alchemy Communications, Inc.'s (the Company or Alchemy) description of its Data Center Colocation Services system (the "System") for the period of November 16, 2016 through November 15, 2017 (the "Period") and the suitability of the design and operating effectiveness of controls to meet the applicable Trust Services Principles (TSP) criteria of Security and Availability as set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. The description indicates that certain trust services criteria can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organizations' Responsibilities

Beginning in section II of the description, the Company has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related TSP of Security and Availability stated in the description. The Company is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, selecting the TSP being reported on and stating the applicable TSP and related controls in the description of the Company's System, identifying any applicable TSP criteria relevant to the principle being reported on that have been omitted from the description and explaining the reason for the omission, designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable TSP.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria. We conducted our examination 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 fairly presented and the controls were suitably designed and operating effectively throughout the Period to meet the applicable trust services criteria.

An examination of a description of a service organization's System and the suitability of the design and operating effectiveness of the service organization's controls involve performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria.

Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in the Company's assertion in section II,

a. management's description of the Company's System fairly presents the Company's System that was designed and implemented throughout the Period,

b. the controls related to the applicable trust services criteria were suitably designed to provide reasonable assurance that those criteria would be met if the controls operated effectively throughout the Period and user entities applied the complementary user entity controls contemplated in the design of the Company's controls throughout the Period,

c. the controls the service auditor tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the Period.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in section IV.

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, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Assure Professional, LLC

Assure Professional, LLC
Green Bay, WI
November 20, 2017

SECTION II – MANAGEMENTS ASSERTIONS

Alchemy™
COMMUNICATIONS, INC.

Management Assertions Letter

We have prepared description of Alchemy Communications, Inc.'s (the "Company") Data Center Colocation Services system (the "System") for the Period November 16, 2016 to November 15, 2017 (the "Period"), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.26-1.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Company's System, particularly System controls intended to meet the criteria for the Security and Availability principles set forth in *TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the Company's System throughout the Period, based on the following description criteria:

i. The description contains the following information

1) the types of services provided

2) the components of the System used to provide the services, which are the following:

- Infrastructure – The physical and hardware components of a system (facilities, equipment, and networks).
- Software – The programs and operating software of a system (systems, applications, and utilities).
- People – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- Procedures – The automated and manual procedures involved in the operation of a system
- Data – The information used and supported by a system (transaction streams, files, databases, and tables).

3) the boundaries or aspects of the System covered by the description

4) how the System captures and addresses significant events and conditions

5) the process used to prepare and deliver reports and other information to user entities and other parties

6) for each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's System

7) any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons therefore

8) other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

9) relevant details of changes to the Company's System during the period covered by the description

ii. The description does not omit or distort information relevant to the Company's System while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs

b. The controls stated in the description were suitably designed throughout the Period to meet the applicable trust services criteria

c. The controls stated in the description operated effectively throughout the Period to meet the applicable trust services criteria.

By:

Title CEO

November 20, 2017

SECTION III – MANAGEMENTS DESCRIPTION OF THE SERVICE ORGANIZATION’S SYSTEM

Company Background and Services

Alchemy Communications, Inc. ("Alchemy" or the "Company") was established in 1995 and is incorporated in the State of California. Alchemy provides Web hosting, colocation, Internet connectivity, data center managed services, Web video streaming services, cloud computing services, and digital marketing solutions. The Company's Internet data center product offerings enable entities to have their Web servers and Web streaming offerings online and working continuously. Alchemy provides its clients with site maintenance and services.

Alchemy is headquartered in Los Angeles, California. Alchemy offers the following services:

- Data Center Colocation
- Internet Connectivity
- Point-to-Point Connectivity
- Continuous Managed Services
- Network Services
- Security Services
- Storage Services
- Reporting Streaming Services
- Custom Information Technology (IT) Solutions
- Cloud Computing Services

Network Operations Center (NOC)

Alchemy employs system administrators and network engineers in its NOC. These staff members are on duty continuously. They constantly monitor Alchemy's network and physical well-being and take immediate action when a problem is detected.

Monitoring for customers includes:

- Continuous onsite technical support
- Access to web-based trouble ticketing system
- 24-hour service/upgrade response time
- Enhanced server/network monitoring
- Connectivity monitoring
- Software Services Monitoring
  - Apache, Simple Mail Transport Protocol (SMTP), File Transfer Protocol (FTP), POP3, etc.
  - Enhanced Package Support
  - Disk space
  - Load/Central Processing Unit (CPU)
  - Processing integrity (credit card processing, etc.) Historical trend reporting Space maintenance (cleans and maintains space weekly)
  - Online, real-time bandwidth reports

Streaming Services

Alchemy offers its customers a full-service video streaming and Web audio streaming offering. Alchemy provides its customers live Webcasting, and video and audio on-demand offerings. Live Webcasting includes both live events and 24-hour per day streaming services such as continuous radio broadcasts. On-demand services allow Alchemy customers to store video and audio clips on its network and to make them available to end-users through their Web sites. Alchemy's network is designed to deliver uninterrupted streaming to its clients' Web sites.

Alchemy's streaming services include:

- Storage - Alchemy offers a complete storage solution for streaming content.
- Encoding - Alchemy offers encoding and compression services to its customers through its internal staff and through a subcontracting relationship. Alchemy offers encoding in a number of digital formats, including .AVI, .JPEG, Microsoft® Windows Media PlayerTM, Real Networks® Real PlayerTM, and Apple® QuicktimeTM.
- Web Site Integration - Alchemy offers simple integration of streaming content to its clients' Web sites.
- Streaming - Alchemy offers live and on-demand streaming of video and audio content over its dedicated network of servers. By purchasing Internet connectivity for its streaming services from multiple carriers, and by using optimizing load balancing techniques, Alchemy is able to offer its customers a quality of service that would be cost prohibitive for many customers to try to replicate on their own.
- Detailed Reporting - Clients can monitor streaming usage from customizable reports that allow the customer to make better informed business decisions.

System Description

The SOC 2 examination covers the operation of Alchemy's Information Technology Environment (IT Environment). The IT Environment operation includes the data center operations, server and network administration, disaster recovery, physical and logical security, and change management processes.

The IT Environment is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, technical support, users, and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, and databases)

The following sections of this description define each of these five components:

INFRASTRUCTURE

The IT Environment infrastructure is comprised of three data centers located in Southern California in downtown Los Angeles, southwest Los Angeles [near Los Angeles Airport (LAX)], and Irvine. Designed to be independent of each other, each data center is configured with redundant uninterruptable power supplies (UPS), generators, and Internet connectivity. All three data centers are connected via a 320-gigabit capacity metro Ethernet ring with a point of presence at One Wilshire carrier hotel, which Alchemy operates using Dense Wavelength Division Multiplexing (DWDM) equipment.

Each facility houses internal servers, networking equipment, and data storage devices that collectively support the Alchemy day to day operations. Each data center is also staffed with IT personnel to support data center operations.

The accompanying SOC 2 examination report covers Alchemy's data center operations and supporting services in the following areas:

- Internal servers
- Network services
- System support services
- Backup and disaster recovery
- Physical and logical security
- Colocation services

Alchemy's data centers house the operating system platforms (Windows, UNIX, LINUX based) and networking components (routers, switches, firewalls) supporting data center operations and services. The roles of the systems/services include: Active Directory services, application servers, backup/recovery services, database servers, development servers, DNS services, FTP services, mail servers, monitoring systems, networking systems, NocWare application servers, statistics services, and Web servers.

SOFTWARE

Software utilized by Alchemy personnel to manage and support the IT Environment includes:

- Backup management
- System monitoring
- Job scheduling, processing, and monitoring
- Network monitoring
- Security monitoring
- Biometric and Keycard applications
- Change management
- Support ticketing system

Alchemy's IT Environment described herein does not include application software supporting the technology solutions provided by Alchemy to individual clients.

PEOPLE

Under the direction of the Chief Executive Officer (CEO), Alchemy is organized into three departments:

- Sales and Marketing
- Network Operations
- Accounting and Human Resources (HR)

The CEO, as well as the heads of these three departments, each has many years of industry experience and each have been with Alchemy for over ten years. Furthermore, Network Operations has the following three divisions: IT, Development, Facilities Management and Administration.

IT personnel provide the following core support services over the Alchemy IT Environment components above:

- Systems and network monitoring
- Security Database administration
- Disaster recovery
- Backup operations
- Network management
- Application change management
- Infrastructure change management
- Customer support
- Internal desktop support

In order to provide these services, IT is divided into three functional areas.

Below is a brief description of each of these functional areas:

- Network - Provides network and communication services for both Alchemy's internal network and Customers.
- System Administration - Provides system and IT services for Alchemy systems.
- NOC Support - Provides system and IT services for customers as well as company personnel help desk support.

PROCEDURES

Alchemy has documented policies and procedures to support the operations and controls over its IT Environment.

Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- System security administration
- Server security configuration
- Computer operations
- Network operations
- Disaster recovery planning
- Change management

- Incident/Problem management
- Physical security
- Tape back-up and offsite storage

DATA

Access to data is limited to authorized personnel in accordance with the Company's security policies. IT is also responsible for the overall availability of data, including system backups, monitoring of data processing and file transmissions as well as identifying and resolving problems. The data Alchemy obtains is usually sensitive to each client. It contains login, server, network, and application information for the client.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Control Activities and Monitoring Activities

ADDITIONAL ELEMENTS OF THE CONTROL ENVIRONMENT

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at Alchemy is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Alchemy places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under Company policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Alchemy has programs and policies designed to promote and ensure the integrity and ethical values in its environment.

Alchemy desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Alchemy developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by HR policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated the Company's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds Alchemy standards.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. Alchemy's management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

The Company is led by a team of senior executives that assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company's goal to deliver client service.

Executive Management is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, client acquisition, market positioning, and Company growth.

Standard Operating Controls

Alchemy management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Alchemy has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. Alchemy conducts pre-employment reference checks from information provided on the employment application. Additionally, HR conducts background investigations relating to past employment history and criminal activity.

Alchemy invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with the Company's organization, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence.

Audit

Alchemy management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

Alchemy has a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect the Company's ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies. Management maintains risk plans and updates them at least annually.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The management team, including the CEO, Chief Financial Officer, and the Vice President of Information Systems, meets regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications. The Company placed into operation the following teams that facilitate identification of relevant risks to the achievement objectives.

Executive Management Team - As a component of its periodic meetings, the Executive Management Team discusses business interruption issues, process improvement, regulatory requirements, compliance, as well as staffing and process change management.

IT Team - The team holds periodic project management meetings covering all aspects of the technology organization. The general theme in IT meetings is to lower cost-of-ownership, reduce risks, and improve on technology investments to provide an ongoing stable and secure IT environment. The team supports the change management process. This process includes the analysis of change (including risks), approval, assignment, development, and implementation of all requested changes.

The Company maintains security policies and communicates them to staff to ensure that individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Information and Communication

Alchemy is focused on the satisfaction of its user organizations and associates, as well as the quality of its service delivery. To ensure that these priorities are continually achieved, Alchemy has implemented formal policies and procedures that address critical operational processes, HR, and information systems. Alchemy's management believes that the internal controls contained in these policies and procedures are critical to effectively running the business operations.

Alchemy has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicate significant events in a timely manner. Employee manuals are provided upon hire that communicate all relevant policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs.

The communication system between senior management and Operations Sr. Staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Periodic department meetings between each manager and their staff are held to discuss new Company policies and procedures and other business issues. Staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of Alchemy.

Trust Services Criteria and Related Controls

The Company's trust services criteria and related control activities are included in Section IV of this report to eliminate the redundancy that would result from listing them here in Section III and repeating them in Section IV. Although the trust services criteria and related control activities are included in Section IV, they are, nevertheless, an integral part of Alchemy's description of controls.

Monitoring

Management monitors internal controls as part of normal business operations. Alchemy uses a series of management reports and processes to monitor the results of the various business processes. The management team regularly reviews reports and logs, records, and resolves all exceptions to normal processing activities.

The Company uses software to track user and customer requests, which are maintained in a system and tracked until completion. Management performs regular reviews of tasks assigned to their departments. Tasks that are not addressed in a timely manner are manually escalated and resolved.

Complementary Controls at User Organizations

The Company's colocation system is designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at Alchemy.

User auditors should consider whether or not the following controls are implemented at user organizations:

- Customers are required to notify Alchemy of all additions, removals, or changes to customer employees with authorized data center physical access.
- Customers are responsible for the selection, use, and compatibility of hardware and software not provided by Alchemy.
- Customers are responsible for the installation, operation, and maintenance of hardware and software installed in the data center when such hardware and software installation, operation, and maintenance is not provided by Alchemy.
- Customers utilizing an authorized caller list for problem management are required to ensure that the authorized caller list remains up-to-date.
- Customers are responsible for developing, maintaining, and testing their own business continuity plan (BPC) or for contracting with Alchemy for its BCP services.
- Customers are responsible for the security and integrity of their transmission facilities, operating facilities, and equipment that are used to access facilities provided by Alchemy.
- Customers must notify Alchemy in advance of any equipment or other shipments they will be sending or receiving.
- Customers are responsible for the transmission and reception of all data and transactions initiated through their Web sites.

- Customers are responsible for discharging all duties to remain in compliance with their agreements with Alchemy.
- Customers are responsible for ensuring that the current configuration of their managed device is in compliance with their requirements document.
- Customers are responsible for having procedures in place which ensure data is backed up or contracting with Alchemy to perform these services.
- Custom monitoring conditions and actions must be specified by the customer and implemented collaboratively with Alchemy provisioning staff.
- Customer is responsible for keeping current with Alchemy's Acceptable Use Policy which is posted on-line in NocWare.
- Customers are responsible for keeping their access control list in NocWare up to date.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Providing data center colocation and managed services for customers by Alchemy covers only a portion of the overall internal control structure of each customer. The Company products and services were not designed to be the only control component in the internal control environment.

Additional control procedures require implementation at the customer level. It is not feasible for all of the control objectives relating to providing data center colocation and managed services to be fully achieved by Alchemy. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV – INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

TRUST SERVICE PRINCIPLES AND RELATED CRITERION

Trust Services Principle – Common Criteria
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to Security and Availabilty.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	Alchemy has an organizational chart that defines the Company's reporting relationships.	Inspected the organizational charts and conducted inquiry of management to determine that documentation was in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No Exceptions Noted.
	The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational charts, sample job descriptions and conducted inquiry of management to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.

Trust Services Principle – Common Criteria
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to Security and Availabilty.		
	The Company has a well defined Departmental Organizational chart with reporting lines and position of various department heads in a hierarchy.	Inspected the department organizational chart to determine that the Company had a well defined Departmental Organizational chart with reporting lines and positions of various department heads in a hierarchy.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational charts, sample job descriptions and conducted inquiry of management to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted.
	Company policies are reviewed annually, updated, and approved by management to remain current.	Inspected in scope policies to determine that company policies were reviewed, updated, and approved by management within the previous twelve months.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting Security and Availabilty and provides resources necessary for personnel to fulfill their responsibilities.		
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.
	New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities.	For selected sample of new hires, inspected the hiring checklist and conducted inquiry of management to determine that new hire checklists were used to ensure that new staff receive the appropriate level of access to information systems and facilities.	No Exceptions Noted.
	During the hiring process, a background check is performed on potential employees before they begin employment with the Company.	For selected sample of new hires, inspected the background authorizations and conducted inquiry of management to determine that during the hiring process, a background check was performed on potential employees before they began employment with the Company.	No Exceptions Noted.
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting Security and Availabilty and provides resources necessary for personnel to fulfill their responsibilities.		
	The Company cross trains employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	Inspected the employee roles listing the individuals trained to perform the job function and conducted corroborative inquiry of management to determine that the Company cross trained employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC1.0	Common Criteria Related to Organization and Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to Security and Availabilty.		
	The Company has established the Rules of Conduct that guides employees on the Company's principles and conduct.	Inspected the Rules of Conduct and conducted inquiry of management to determine that documentation was in place to guide employees on the organization's ethical principles and conduct.	No Exceptions Noted.
	During the hiring process, a background check is performed on potential employees before they begin employment with the Company.	For selected sample of new hires, inspected the background authorizations and conducted inquiry of management to determine that during the hiring process, a background check was performed on potential employees before they began employment with the Company.	No Exceptions Noted.
	An Acceptable Use Policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	Inspected the Company Acceptable Use Policy as contained within the Security Policies to determine that an Acceptable Use Policy was in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	No Exceptions Noted.
	Employees must sign a confidentiality agreement as acknowledgment not to disclose proprietary or confidential information.	For selected sample of 3 new hires, inspected the confidentiality agreement and conducted inquiry of management to determine that employees were required to sign the agreement not to disclose proprietary or confidential information.	No Exceptions Noted.
	There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies.	Inspected the Disciplinary Procedures and conducted inquiry of management to determine that there was a formal policy for employees who were suspected of rule infractions or violations of company policies.	No Exceptions Noted.

CC2.0	Common Criteria Related to Communications		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.		
	A Network Diagram is in place and update when infrastructure is updated.	Inspected the network diagram to determine that a network topology is documented and updated regularly.	No Exceptions Noted.
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.
	A description of the system is posted on the Company's Public Web Site and is available to users.	Inspected the Corporate website to determine that a description of the system is posted on the Company's Public Web Site and was available to users.	No Exceptions Noted.
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.
	The Company has documented standard operating procedures to communicate the responsibilities and requirements for delivery of services.	Inspected the Escalation and Standard Procedures Policy and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.		
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.
	Employees must sign a statement confirming acknowledgment of the IT Security Policies.	For selected sample of new hires, inspected the acknowledgments and conducted inquiry of management to determine that employees must sign a statement confirming acknowledgment of all policies and procedures in the IT Security Policies.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)

Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC2.2	The entity's Security and Availabilty commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	The Company has established the Rules of Conduct that guides employees on the Company’s principles and conduct.	Inspected the Rules of Conduct and conducted inquiry of management to determine that documentation was in place to guide employees on the organization’s ethical principles and conduct.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.
	A description of the system is posted on the Company's Public Web Site and is available to users.	Inspected the Corporate website to determine that a description of the system is posted on the Company's Public Web Site and was available to users.	No Exceptions Noted.
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.2	The entity's Security and Availabilty commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.		
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.
	Employees must sign a statement confirming acknowledgment of the IT Security Policies.	For selected sample of new hires, inspected the acknowledgments and conducted inquiry of management to determine that employees must sign a statement confirming acknowledgment of all policies and procedures in the IT Security Policies.	No Exceptions Noted.
	A Privacy Policy is in place and communicated to users on the entity's web site.	Inspected the Privacy Policy as presented on the Company's web site to determine that a Privacy Policy was in place and communicated to users on the entity's web site.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	The Company has established the Rules of Conduct that guides employees on the Company's principles and conduct.	Inspected the Rules of Conduct and conducted inquiry of management to determine that documentation was in place to guide employees on the organization's ethical principles and conduct.	No Exceptions Noted.
	Company policies are reviewed annually, updated, and approved by management to remain current.	Inspected in scope policies to determine that company policies were reviewed, updated, and approved by management within the previous twelve months.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the Job Description for the Director of IT and conducted corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.		
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.
	The Company has documented standard operating procedures to communicate the responsibilities and requirements for delivery of services.	Inspected the Escalation and Standard Procedures Policy and conducted corroborative inquiry of management to determine that standard operating procedures were documented and in place.	No Exceptions Noted.
	An Acceptable Use Policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	Inspected the Company Acceptable Use Policy as contained within the Security Policies to determine that an Acceptable Use Policy was in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	No Exceptions Noted.
	Employees must sign a confidentiality agreement as acknowledgment not to disclose proprietary or confidential information.	For selected sample of 3 new hires, inspected the confidentiality agreement and conducted inquiry of management to determine that employees were required to sign the agreement not to disclose proprietary or confidential information.	No Exceptions Noted.
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.		
	Employees must sign a statement confirming acknowledgment of the IT Security Policies.	For selected sample of new hires, inspected the acknowledgments and conducted inquiry of management to determine that employees must sign a statement confirming acknowledgment of all policies and procedures in the IT Security Policies.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.
	A Privacy Policy is in place and communicated to users on the entity's web site.	Inspected the Privacy Policy as presented on the Company's web site to determine that a Privacy Policy was in place and communicated to users on the entity's web site.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security and Availabilty of the system, is provided to personnel to carry out their responsibilities.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	Roles and Responsibilities are defined in written job descriptions and communicated to key staff responsible for Security and Availability.	Inspected sample job descriptions and conducted inquiry of management to determine they were in place and described the roles and responsibilities of the position.	No Exceptions Noted.
	Risk Committee meetings are held periodically to monitor the controls of the company.	Inspected results of the risk review and conducted inquiry of management to determine that the Risk Committee meetings were held at least annually to monitor the controls of the company.	No Exceptions Noted.
	A description of the system is posted on the Company's Public Web Site and is available to users.	Inspected the Corporate website to determine that a description of the system is posted on the Company's Public Web Site and was available to users.	No Exceptions Noted.
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security and Availabilty of the system, is provided to personnel to carry out their responsibilities.		
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.
	The Company cross trains employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	Inspected the employee roles listing the individuals trained to perform the job function and conducted corroborative inquiry of management to determine that the Company cross trained employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	No Exceptions Noted.
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Data Destruction and Technology Equipment Disposal Policy section as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.5	Internal and external users have been provided with information on how to report Security and Availabilty failures, incidents, concerns, and other complaints to appropriate personnel.		
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.
	Staff are given Security Awareness training during their new hire orientation and are then updated on a annual basis.	For selected sample of new hires, inspected the training acknowledgments and conducted inquiry of management to determine that staff were given Security Awareness training during their new hire orientation and then updated on a annual basis.	No Exceptions Noted.
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected sample alerts and conducted inquiry of management to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.5	Internal and external users have been provided with information on how to report Security and Availabilty failures, incidents, concerns, and other complaints to appropriate personnel.		
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Data Destruction and Technology Equipment Disposal Policy section as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC2.0	Common Criteria Related to Communications (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to Security and Availabilty are communicated to those users in a timely manner.		
	Management meetings are held on a regular basis to discuss operational issues.	Inspected screenshots of the schedule of meetings to determine that management meetings were held on a regular basis to discuss operational issues.	No Exceptions Noted.
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected screen prints of the application and conducted inquiry of management to determine that the Company had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted.
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	Changes are authorized and scheduled when testing is complete.	For selected sample of change tickets, inspected the change process and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted.
	Hardware and software maintenance for networking equipment is scheduled and managed according to the change management process, user who may be affected are notified prior to a planned event.	For selected sample of infrastructure change tickets, inspected the task scheduling requirements and conducted a corroborative inquiry of management to determine that hardware and software maintenance for networking equipment was scheduled and managed according to the change management process.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the Job Description for the Director of IT and conducted corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	The Company has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Access Policy and Procedures section as contained within the Security Policies document and observed the physical security controls during onsite procedures to determine that the Company had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted.
	Backup tapes are securely destroyed when their useful life expires. The destruction process physically destroys the media to prevent retrieval of data.	Inspected the Data Destruction and Technology Equipment Disposal Policy section as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that backup tapes were securely destroyed when their useful life expires.	No Exceptions Noted.
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	The Company subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected screen prints of the security bulletin emails and conducted a corroborative inquiry of management to determine that the Company subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted.
	The clocks of all relevant information processing systems within the Company are synchronized with an accurate time source.	For selected sample of servers, inspected the NPT settings and conducted inquiry of management to determine that the system clocks of all relevant information processing systems within the Company were synchronized with an accurate time source.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected screen prints of the application and conducted inquiry of management to determine that the Company had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted.
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	For the selected quarter, inspected screen prints of the quarterly review and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	The firewall is configured to automatically terminate authenticated sessions to the firewall if predefined inactivity thresholds are exceeded.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to automatically terminate authenticated sessions to the firewall if predefined inactivity thresholds were exceeded.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Availabilty commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the plan revision date and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	The Company maintains an Information Security Policy that describes the policies and procedures for ensuring system security and availability objectives are met. The Information Security Policy is reviewed and acknowledged by the IT Director annually.	Inspected the Security Policies and policy approval to determine that it was in place and described the security posture and practices of the Company.	No Exceptions Noted.
	The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational charts, sample job descriptions and conducted inquiry of management to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted.
	The Company has an Network Operation Center Policies and Procedures that describes management's philosophy, operating style, and provides guidance to employees.	Inspected the Employee Handbook and conducted inquiry of management to determine that management's philosophy and operating style were documented and communicated to employees.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	The Company has established the Rules of Conduct that guides employees on the Company's principles and conduct.	Inspected the Rules of Conduct and conducted inquiry of management to determine that documentation was in place to guide employees on the organization's ethical principles and conduct.	No Exceptions Noted.
	Company policies are reviewed annually, updated, and approved by management to remain current.	Inspected in scope policies to determine that company policies were reviewed, updated, and approved by management within the previous twelve months.	No Exceptions Noted.
	The Company maintains insurance policies to mitigate losses and transfer certain identified risks.	Inspected the insurance declarations and conducted inquiry of management to determine that the Company maintained insurance policies to mitigate losses and transfer certain identified risks.	No Exceptions Noted.
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the Job Description for the Director of IT and conducted corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted.
	The Company publishes its IT security policy on its corporate intranet.	Inspected screen prints of the internal corporate web site to determine that the Company published its IT security policy on its corporate intranet.	No Exceptions Noted.
	During the hiring process, a background check is performed on potential employees before they begin employment with the Company.	For selected sample of new hires, inspected the background authorizations and conducted inquiry of management to determine that during the hiring process, a background check was performed on potential employees before they began employment with the Company.	No Exceptions Noted.
	An Acceptable Use Policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	Inspected the Company Acceptable Use Policy as contained within the Security Policies to determine that an Acceptable Use Policy was in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	Employees must sign a confidentiality agreement as acknowledgment not to disclose proprietary or confidential information.	For selected sample of 3 new hires, inspected the confidentiality agreement and conducted inquiry of management to determine that employees were required to sign the agreement not to disclose proprietary or confidential information.	No Exceptions Noted.
	There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies.	Inspected the Disciplinary Procedures and conducted inquiry of management to determine that there was a formal policy for employees who were suspected of rule infractions or violations of company policies.	No Exceptions Noted.
	The Company has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Access Policy and Procedures section as contained within the Security Policies document and observed the physical security controls during onsite procedures to determine that the Company had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted.
	Management maintains documented backup schedules, policies, and procedures.	Inspected the Backup and Restore Policy and Procedures as contained within the Security Policies and conducted inquiry of management to determine that it was and place.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	Policies and procedures are in place for patch management on production systems.	For selected sample of servers, inspected the server patch level, patching procedures and conducted inquiry of management to determine that a patch management process was in place.	No Exceptions Noted.
	The Company subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected screen prints of the security bulletin emails and conducted a corroborative inquiry of management to determine that the Company subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	The clocks of all relevant information processing systems within the Company are synchronized with an accurate time source.	For selected sample of servers, inspected the NPT settings and conducted inquiry of management to determine that the system clocks of all relevant information processing systems within the Company were synchronized with an accurate time source.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	For the selected quarter, inspected screen prints of the quarterly review and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted.
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Observed the nonexistent terminated users accounts and conducted a corroborative inquiry of management to determine that terminated employees' access was revoked.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected screen prints of the firewall interface settings and conducted a corroborative inquiry of management to determine that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.
	The Company has implemented countermeasures to protect against denial of service attacks.	Inspected the Denial Of Service Attack Procedure as contained within Security Policies to determine that the countermeasures to protect against DDOS attacks were in place.	No Exceptions Noted.
	Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information.	Inspected the Acceptable Encryption Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	Management maintains a remote access policy and procedure that provides guidance on Company standards for administering connections to and from remote networks.	Inspected the Remote Access Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Disaster Recovery & Business Continuity Plan and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted.
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the DR test ticket and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted.
	Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents.	Inspected the Data Classification and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the classification of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents.	Inspected the Data Retention Policy as contained within Security Policies and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the retention of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.
	A Privacy Policy is in place and communicated to users on the entity's web site.	Inspected the Privacy Policy as presented on the Company's web site to determine that a Privacy Policy was in place and communicated to users on the entity's web site.	No Exceptions Noted.
	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded or recycled.	Inspected the Data Destruction and Technology Equipment Disposal Policy and conducted a corroborative inquiry of management to determine that all media was physically or logically destroyed rendering all sensitive information unreadable before being discarded or recycled.	No Exceptions Noted.

CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
	Policies and procedures are in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	Inspected the Data Destruction and Technology Equipment Disposal Policy section as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the handling of client information related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the Escalation and Standards Procedures Policy and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC4.0	Common Criteria Related to Monitoring of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to Security and Availabilty, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.		
	Management meetings are held on a regular basis to discuss operational issues.	Inspected screenshots of the schedule of meetings to determine that management meetings were held on a regular basis to discuss operational issues.	No Exceptions Noted.
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	Security walkthroughs are performed daily throughout each shift to monitor and check physical security as well as monitor health status of environmental systems.	Inspected sample of security walkthrough tickets and conducted corroborative inquiry of management to determine that Security walkthroughs were performed daily throughout each shift to monitor and check physical security as well as monitor health status of environmental systems.	No Exceptions Noted.
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC4.0	Common Criteria Related to Monitoring of Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to Security and Availabilty, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.		
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)

Common Criteria to Security and Availabilty

CC4.0	Common Criteria Related to Monitoring of Controls		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to Security and Availabilty, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.		
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the Escalation and Standard Procedures Policy as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Changes to user permissions in the access control system are documented and require management approval.	For selected sample of change requests, inspected the user access ticket and conducted inquiry of management to determine that changes to user permissions in the access control system were documented and required management approval.	No Exceptions Noted.
	Periodic audits of the Access Control System is performed to validate access cards and user access.	For selected quarterly review of the ACS system, inspected the review worksheet and conducted inquiry of management to determine that an ACS audit was performed.	No Exceptions Noted.
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Account Management Policy, the Computing Passwords policy as contained within the Security Policies document to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Network users are authenticated via an authorized network ID and password before being granted access to the network domain.	Inspected screen prints of the AD users and observed the logon process during onsite procedures to determine that network users were authenticated via an authorized network ID and password before begin granted access to the network.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Passwords must conform to minimum requirements as enforced by the network operating system. Password complexity standards are established to enforce control over access control software passwords.	Inspected screen prints of the password settings and conducted a corroborative inquiry of management to determine that network passwords conform to the requirements.	No Exceptions Noted.
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	For the selected quarter, inspected screen prints of the quarterly review and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted.
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Observed the nonexistent terminated users accounts and conducted a corroborative inquiry of management to determine that terminated employees' access was revoked.	No Exceptions Noted.
	User change procedures are in place for the change of access to all systems upon notification of a user role change.	Inspected the User Account Management Policy as contained within the Security Polices document and conducted a corroborative inquiry of management to determine that user profile change procedures were in place.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Remote access to the network requires dual factor authentication.	Inspected screen prints of the dual factor authentication settings and conducted inquiry of management to determine that remote access to the network requires dual factor authentication.	No Exceptions Noted.
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.
	Router and Firewall rules are reviewed every 6 months to ensure settings have not been modified.	Inspected the Network audit checks as contained within the security policies, screen prints of the firewall review closed ticket and conducted a corroborative inquiry of management to determine that Router and Firewall rules were reviewed every 6 months to ensure settings have not been modified.	No Exceptions Noted.
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected screen prints of the site to site VPN configuration settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted.
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions to the corporate network.	Inspected screen prints of the remote user VPN settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to Security and Availabilty. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational charts, sample job descriptions and conducted inquiry of management to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted.
	New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities.	For selected sample of new hires, inspected the hiring checklist and conducted inquiry of management to determine that new hire checklists were used to ensure that new staff receive the appropriate level of access to information systems and facilities.	No Exceptions Noted.
	Management utilizes and retains termination checklists as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	For selected sample of terminations, inspected the termination checklist and conducted inquiry of management to determine that management utilized termination checklists as confirmation of revocation of system and facility access privileges when terminated.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to Security and Availabilty. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Account Management Policy, the Computing Passwords policy as contained within the Security Policies document to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	For the selected quarter, inspected screen prints of the quarterly review and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted.
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Observed the nonexistent terminated users accounts and conducted a corroborative inquiry of management to determine that terminated employees' access was revoked.	No Exceptions Noted.
	User change procedures are in place for the change of access to all systems upon notification of a user role change.	Inspected the User Account Management Policy as contained within the Security Polices document and conducted a corroborative inquiry of management to determine that user profile change procedures were in place.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Visitors are required to check in with the receptionist utilizing a government issued identifications and are escorted for the duration of their visit.	Observed the visitor check in procedures to determine that visitors were required to check in with the receptionist and were escorted for the duration of their visit.	No Exceptions Noted.
	Visitors must sign in and provide a government issued ID prior to issuance of a visitors badge. Visitors badges are for identification only and do not permit access to the facilities.	Observed the visitors check-in proces during onsite procedures to determine that visitors were required to sign the visitor log and were issued a visitor badge which was displayed by the visitor while on the premises.	Exception Noted. LAX Badge printer issue. See table at the end of report
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Account Management Policy, the Computing Passwords policy as contained within the Security Policies document to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Network users are authenticated via an authorized network ID and password before being granted access to the network domain.	Inspected screen prints of the AD users and observed the logon process during onsite procedures to determine that network users were authenticated via an authorized network ID and password before begin granted access to the network.	No Exceptions Noted.
	Passwords must conform to minimum requirements as enforced by the network operating system. Password complexity standards are established to enforce control over access control software passwords.	Inspected screen prints of the password settings and conducted a corroborative inquiry of management to determine that network passwords conform to the requirements.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Remote access to the network requires dual factor authentication.	Inspected screen prints of the dual factor authentication settings and conducted inquiry of management to determine that remote access to the network requires dual factor authentication.	No Exceptions Noted.
	Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information.	Inspected the Acceptable Encryption Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected screen prints of the site to site VPN configuration settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted.
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions to the corporate network.	Inspected screen prints of the remote user VPN settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information.	Inspected the organizational charts, sample job descriptions and conducted inquiry of management to determine that the organization was segregated into separate, logical, and distinct functional areas for the purpose of management and processing of customer information.	No Exceptions Noted.
	New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities.	For selected sample of new hires, inspected the hiring checklist and conducted inquiry of management to determine that new hire checklists were used to ensure that new staff receive the appropriate level of access to information systems and facilities.	No Exceptions Noted.
	Management utilizes and retains termination checklists as confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	For selected sample of terminations, inspected the termination checklist and conducted inquiry of management to determine that management utilized termination checklists as confirmation of revocation of system and facility access privileges when terminated.	No Exceptions Noted.
	Access cards are disabled timely upon receipt of termination notice from the appropriate manager.	For selected sample of terminations, inspected the termination ticket revoking the access card and conducted inquiry of management to determine that an ACS termination's were properly documented and conducted timely.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Account Management Policy, the Computing Passwords policy as contained within the Security Policies document to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Network domain administrator rights are restricted to specific network operations personnel.	Inspected screen prints of the admin members and conducted a corroborative inquiry of management to determine that network administrator rights were restricted to certain authorized personnel as described.	No Exceptions Noted.
	Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities.	For the selected quarter, inspected screen prints of the quarterly review and conducted a corroborative inquiry of management to determine the audits were performed to monitor user access rights assignments.	No Exceptions Noted.
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Observed the nonexistent terminated users accounts and conducted a corroborative inquiry of management to determine that terminated employees' access was revoked.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	User change procedures are in place for the change of access to all systems upon notification of a user role change.	Inspected the User Account Management Policy as contained within the Security Polices document and conducted a corroborative inquiry of management to determine that user profile change procedures were in place.	No Exceptions Noted.
	Direct access to the firewalls is restricted to a predefined set of IP addresses, and communications are encrypted.	Inspected screen prints of the firewall configurations and conducted a corroborative inquiry of management to determine that direct access to the firewall was restricted to a predefined set of IP addresses and that communications were encrypted.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Company has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Access Policy and Procedures section as contained within the Security Policies document and observed the physical security controls during onsite procedures to determine that the Company had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted.
	All entrances to the data center remain locked at all times. Access is restricted and requires multi-factor authentication. Entry is controlled by a proximity card system and/or Biometrics sensors and/or PIN number pad.	Observed the physical access controls during onsite procedures to determine that entry controls were instituted and enforced.	No Exceptions Noted.
	The walls surrounding the data center extend above the drop ceiling tiles all the way to the physical ceiling in order to prevent unauthorized access to restricted areas.	Observed the data center walls during onsite procedures to determine that the walls surrounding the data center extended above the drop ceiling tiles up to the physical ceiling.	No Exceptions Noted.
	Visitors are required to check in with the receptionist utilizing a government issued identifications and are escorted for the duration of their visit.	Observed the visitor check in procedures to determine that visitors were required to check in with the receptionist and were escorted for the duration of their visit.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Visitors must sign in and provide a government issued ID prior to issuance of a visitors badge. Visitors badges are for identification only and do not permit access to the facilities.	Observed the visitors check-in proces during onsite procedures to determine that visitors were required to sign the visitor log and were issued a visitor badge which was displayed by the visitor while on the premises.	Exception Noted. LAX Badge printer issue. See table at the end of report
	Man traps or monitored waiting areas are used in the data center as an additional security measure prior to gaining access to the data center floor.	Observed the man trap and entry procedures during onsite procedures to determine that man traps were used in the data center as an additional security measure prior to gaining access to the data center floor.	No Exceptions Noted.
	Generator Access is controlled by alarm and key lock.	Observed the secured generator areas to determine that access to the generator was restricted to authorized individuals.	No Exceptions Noted.
	Personnel are on duty at the data center facility.	Inspected the NOC personnel schedule, observed the onsite personnel and conducted inquiry of management to determine that personnel were on duty at the data center facility.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The badge access system has been configured with restricted zones for critical areas that require an elevated level of access.	Observed the secure areas during onsite procedures to determine that the badge access system had been configured with restricted zones for critical areas that required an elevated level of access.	No Exceptions Noted.
	Management restricts the ability to create, modify, or delete user badge access privileges to the facility.	Inspected screen prints of the ACS authorized administrators and conducted inquiry of management to determine that management restricted the ability to create, modify, or delete user badge access privileges to the facility.	No Exceptions Noted.
	Surveillance cameras record activities at the facility entrances and other areas within the facility.	Observed the video surveillance cameras during onsite procedures to determine that surveillance cameras recorded activities at the facility entrances and other areas within the facility.	No Exceptions Noted.
	Periodic audits of the Access Control System is performed to validate access cards and user access.	For selected quarterly review of the ACS system, inspected the review worksheet and conducted inquiry of management to determine that an ACS audit was performed.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Access cards are disabled timely upon receipt of termination notice from the appropriate manager.	For selected sample of terminations, inspected the termination ticket revoking the access card and conducted inquiry of management to determine that an ACS termination's were properly documented and conducted timely.	No Exceptions Noted.
	Security walkthroughs are performed daily throughout each shift to monitor and check physical security as well as monitor health status of environmental systems.	Inspected sample of security walkthrough tickets and conducted corroborative inquiry of management to determine that Security walkthroughs were performed daily throughout each shift to monitor and check physical security as well as monitor health status of environmental systems.	No Exceptions Noted.
	Backup media is physically secured while onsite and access is restricted to only authorized personnel.	Observed the secure media during onsite procedures to determine that backup media was secured while on-site and access was restricted to authorized personnel.	No Exceptions Noted.
	Termination procedures are in place for the removal of access to all systems upon notification of the termination.	Observed the nonexistent terminated users accounts and conducted a corroborative inquiry of management to determine that terminated employees' access was revoked.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.6	Logical access security measures have been implemented to protect against Security and Availabilty threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
	Access to modify backup jobs and backup job notification settings is restricted to authorized personnel.	Inspected screen prints of the authorized users and conducted a corroborative inquiry of management to determine that access to make changes to the backup jobs and backup notification settings was restricted to authorized personnel.	No Exceptions Noted.
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected sample alerts and conducted inquiry of management to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted.
	Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards.	Inspected the User Account Management Policy, the Computing Passwords policy as contained within the Security Policies document to determine the policies and procedures had been implemented.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.6	Logical access security measures have been implemented to protect against Security and Availabilty threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
	Remote access to the network requires dual factor authentication.	Inspected screen prints of the dual factor authentication settings and conducted inquiry of management to determine that remote access to the network requires dual factor authentication.	No Exceptions Noted.
	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected screen prints of the firewall interface settings and conducted a corroborative inquiry of management to determine that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No Exceptions Noted.
	A redundant standby firewall is in place and has been configured as a fail-over to the primary firewall.	Inspected screen prints of the standby firewall settings and conducted a corroborative inquiry of management to determine that a redundant firewall was in place and has been configured as a fail over.	No Exceptions Noted.
	Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel.	Inspected screen prints of the authorized users and conducted a corroborative inquiry of management to determine to determine the credentials were required to administer the devices.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.6	Logical access security measures have been implemented to protect against Security and Availabilty threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Network Address Translation (NAT) services are enabled on the network firewalls.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that NAT services were enabled on the network firewall.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.
	The Company has implemented countermeasures to protect against denial of service attacks.	Inspected the Denial Of Service Attack Procedure as contained within Security Policies to determine that the countermeasures to protect against DDOS attacks were in place.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.6	Logical access security measures have been implemented to protect against Security and Availabilty threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
	Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information.	Inspected the Acceptable Encryption Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected screen prints of the site to site VPN configuration settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted.
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions to the corporate network.	Inspected screen prints of the remote user VPN settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted.
	Management maintains a remote access policy and procedure that provides guidance on Company standards for administering connections to and from remote networks.	Inspected the Remote Access Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to Security and Availabilty.		
	Backup sets containing target data utilizes encryption to prevent unauthorized access.	Inspected screen prints of the backup encryption settings and conducted a corroborative inquiry of management to determine that backup sets were encrypted to restrict access.	No Exceptions Noted.
	Backup media is kept in steel locked containers when transported between data center locations.	Observed the locked container during onsite procedures and conducted inquiry of management to determine that backup media was secured in a locked container while being transported between data centers.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Wireless access points exist on a network that is external to production systems. WPA2 encryption is used.	Observed the guest wireless network during onsite procedures and conducted a corroborative inquiry of management to determine that encryption was in place on the wireless network.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to Security and Availabilty.		
	Router and Firewall rules are reviewed every 6 months to ensure settings have not been modified.	Inspected the Network audit checks as contained within the security policies, screen prints of the firewall review closed ticket and conducted a corroborative inquiry of management to determine that Router and Firewall rules were reviewed every 6 months to ensure settings have not been modified.	No Exceptions Noted.
	Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information.	Inspected the Acceptable Encryption Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.
	Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network using SSL or IPSec.	Inspected screen prints of the VPN settings and conducted a corroborative inquiry of management to determine that VPN is in use.	No Exceptions Noted.
	Site to site VPN connections are utilized over public networks for encrypting sensitive information to ensure the privacy and integrity of the data passing over the public network.	Inspected screen prints of the site to site VPN configuration settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized for the secure transmission of data.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to Security and Availabilty.		
	Remote user VPN connections are utilized by staff to establish encrypted communication sessions to the corporate network.	Inspected screen prints of the remote user VPN settings and conducted a corroborative inquiry of management to determine that the connections were in place and utilized by staff for establishing encrypted communication sessions to the corporate network.	No Exceptions Noted.
	Secure communication tunnels are in place for file transfers requiring encryption to the company's servers through the use of SSL encryption.	Inspected screen prints of the security certificates and conducted a corroborative inquiry of management to determine that the server was being utilized as described.	No Exceptions Noted.
	Management maintains a remote access policy and procedure that provides guidance on Company standards for administering connections to and from remote networks.	Inspected the Remote Access Policy as contained within the Security Policies and conducted a corroborative inquiry of management to determine the policies and procedures had been implemented.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected screen prints of the backup application and conducted inquiry of management to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted.
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	The Company subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected screen prints of the security bulletin emails and conducted a corroborative inquiry of management to determine that the Company subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Network security event logging is configured to log specific events on the network.	Inspected sample reports of the security monitoring and logging application and conducted a corroborative inquiry of management to determine that network audit settings were configured to log specific security events on the network.	No Exceptions Noted.
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC5.0	Common Criteria Related to Logical and Physical Access Controls (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.1	Vulnerabilities of system components to Security and Availabilty breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	A Network Diagram is in place and update when infrastructure is updated.	Inspected the network diagram to determine that a network topology is documented and updated regularly.	No Exceptions Noted.
	The Company maintains insurance policies to mitigate losses and transfer certain identified risks.	Inspected the insurance declarations and conducted inquiry of management to determine that the Company maintained insurance policies to mitigate losses and transfer certain identified risks.	No Exceptions Noted.
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	Security Planning and Maintenance responsibilities have been delegated.	Inspected the Job Description for the Director of IT and conducted corroborative inquiry of management to determine that responsibility for Security Planning and Maintenance had been delegated.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.1	Vulnerabilities of system components to Security and Availabilty breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected sample alerts and conducted inquiry of management to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted.
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.1	Vulnerabilities of system components to Security and Availabilty breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Company subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected screen prints of the security bulletin emails and conducted a corroborative inquiry of management to determine that the Company subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected screen prints of the application and conducted inquiry of management to determine that the Company had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted.
	Network security event logging is configured to log specific events on the network.	Inspected sample reports of the security monitoring and logging application and conducted a corroborative inquiry of management to determine that network audit settings were configured to log specific security events on the network.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.1	Vulnerabilities of system components to Security and Availabilty breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.1	Vulnerabilities of system components to Security and Availabilty breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Company has implemented countermeasures to protect against denial of service attacks.	Inspected the Denial Of Service Attack Procedure as contained within Security Policies to determine that the countermeasures to protect against DDOS attacks were in place.	No Exceptions Noted.
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Disaster Recovery & Business Continuity Plan and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted.
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the plan revision date and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted.
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the Escalation and Standards Procedures Policy and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted.
	Support staff are available 24x7x365.	Inspected the support schedule and conducted a corroborative inquiry of management to determine that support staff were available after business hours.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies.	Inspected the Disciplinary Procedures and conducted inquiry of management to determine that there was a formal policy for employees who were suspected of rule infractions or violations of company policies.	No Exceptions Noted.
	The Company has policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	Inspected the Physical Access Policy and Procedures section as contained within the Security Policies document and observed the physical security controls during onsite procedures to determine that the Company had policies and procedures governing physical security controls that limit access to the facility to authorized individuals.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	All entrances to the data center remain locked at all times. Access is restricted and requires multi-factor authentication. Entry is controlled by a proximity card system and/or Biometrics sensors and/or PIN number pad.	Observed the physical access controls during onsite procedures to determine that entry controls were instituted and enforced.	No Exceptions Noted.
	Surveillance cameras record activities at the facility entrances and other areas within the facility.	Observed the video surveillance cameras during onsite procedures to determine that surveillance cameras recorded activities at the facility entrances and other areas within the facility.	No Exceptions Noted.
	Surveillance camera recordings are maintained for a certain number of days, allowing the capability for ad hoc review and investigations.	Observed the video recordings during onsite procedures to determine surveillance camera recordings were maintained for a certain number of days, allowing the capability for ad hoc review and investigations.	No Exceptions Noted.
	Periodic audits of the Access Control System is performed to validate access cards and user access.	For selected quarterly review of the ACS system, inspected the review worksheet and conducted inquiry of management to determine that an ACS audit was performed.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	The Company subscribes to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	Inspected screen prints of the security bulletin emails and conducted a corroborative inquiry of management to determine that the Company subscribed to security bulletins and notices for newly discovered vulnerabilities in order to identify patches to be applied.	No Exceptions Noted.
	User requirements for informing the Company about breaches is documented in the service level agreements and the Client Acceptable Use Policy.	Inspected the Security section as documented in the Client Acceptable User Policy to determine that user requirements for informing the Company about breaches was communicated to users.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	An application is used to identify authorized and unauthorized devices connecting to the network.	Inspected screen prints of the application and conducted inquiry of management to determine that the Company had automated applications to identify authorized and unauthorized devices connecting to the network.	No Exceptions Noted.
	Network security event logging is configured to log specific events on the network.	Inspected sample reports of the security monitoring and logging application and conducted a corroborative inquiry of management to determine that network audit settings were configured to log specific security events on the network.	No Exceptions Noted.
	Systems Logs and Audit Trails re restricted and protected from unauthorized access and alteration.	Inspected screen prints of the logging application and conducted a corroborative inquiry of management to determine that system logs and audit trails were protected from unauthorized access and were backed up.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	An Intrusion Prevention Systems (IPS) is utilized to monitor the network for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screen prints of the firewall IPS settings and conducted a corroborative inquiry of management to determine that a IPS was in place, monitoring the network continuously, and provided alert to administrators.	No Exceptions Noted.
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	The Company has implemented countermeasures to protect against denial of service attacks.	Inspected the Denial Of Service Attack Procedure as contained within Security Policies to determine that the countermeasures to protect against DDOS attacks were in place.	No Exceptions Noted.
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the Escalation and Standards Procedures Policy and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted.
	Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected screen prints of the ticketing application and conducted a corroborative inquiry of management to determine that the tickets were created, worked, and documented as described.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)

Common Criteria to Security and Availabilty

CC6.0	Common Criteria Related to System Operations (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC6.2	Security and Availabilty incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the Escalation and Standard Procedures Policy as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted.
	Incoming Support tickets are prioritized based on the level of criticality and addressed by highest impacting request to ensure minimal disruption of service to users.	For selected sample of support tickets, inspected the support ticket priority and conducted a corroborative inquiry of management to determine that tickets were prioritized based on level of criticality and addressed by highest impacting request to minimize disruption of services.	No Exceptions Noted.

CC7.0	Common Criteria Related to Change Management		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
CC7.1	The entity's commitments and system requirements, as they relate to Security and Availabilty, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.		
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	Changes to the production environment are documented in the ticketing system and a work order is created.	For selected sample of infrastructure changes, inspected the change ticket and conducted a corroborative inquiry of management to determine that changes were logged in a ticketing system.	No Exceptions Noted.
	The Change review board or IT Management must approve proposed changes that affect the production environment.	For selected sample of infrastructure change tickets, inspected the ticket approval and conducted a corroborative inquiry of management to determine that changes were properly reviewed and approved.	No Exceptions Noted.
	Changes are authorized and scheduled when testing is complete.	For selected sample of change tickets, inspected the change process and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted.
	Hardware and software maintenance for networking equipment is scheduled and managed according to the change management process, user who may be affected are notified prior to a planned event.	For selected sample of infrastructure change tickets, inspected the task scheduling requirements and conducted a corroborative inquiry of management to determine that hardware and software maintenance for networking equipment was scheduled and managed according to the change management process.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC7.0	Common Criteria Related to Change Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to Security and Availabilty.		
	Policies and procedures are in place for patch management on production systems.	For selected sample of servers, inspected the server patch level, patching procedures and conducted inquiry of management to determine that a patch management process was in place.	No Exceptions Noted.
	Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents.	Inspected the Data Classification and conducted a corroborative inquiry of management to determine that policies were in place to guide personnel on their responsibility for the classification of documents and data related to the secure storage and destruction of sensitive data and documents.	No Exceptions Noted.
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	Changes to the production environment are documented in the ticketing system and a work order is created.	For selected sample of infrastructure changes, inspected the change ticket and conducted a corroborative inquiry of management to determine that changes were logged in a ticketing system.	No Exceptions Noted.

CC7.0	Common Criteria Related to Change Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Change review board or IT Management must approve proposed changes that affect the production environment.	For selected sample of infrastructure change tickets, inspected the ticket approval and conducted a corroborative inquiry of management to determine that changes were properly reviewed and approved.	No Exceptions Noted.
	Changes are authorized and scheduled when testing is complete.	For selected sample of change tickets, inspected the change process and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted.
	Hardware and software maintenance for networking equipment is scheduled and managed according to the change management process, user who may be affected are notified prior to a planned event.	For selected sample of infrastructure change tickets, inspected the task scheduling requirements and conducted a corroborative inquiry of management to determine that hardware and software maintenance for networking equipment was scheduled and managed according to the change management process.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC7.0	Common Criteria Related to Change Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected sample alerts and conducted inquiry of management to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted.
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	Systems Logs and Audit Trails re restricted and protected from unauthorized access and alteration.	Inspected screen prints of the logging application and conducted a corroborative inquiry of management to determine that system logs and audit trails were protected from unauthorized access and were backed up.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC7.0	Common Criteria Related to Change Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to Security and Availabilty.		
	The Change review board or IT Management must approve proposed changes that affect the production environment.	For selected sample of infrastructure change tickets, inspected the ticket approval and conducted a corroborative inquiry of management to determine that changes were properly reviewed and approved.	No Exceptions Noted.
	Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.	Inspected the Escalation and Standards Procedures Policy and conducted a corroborative inquiry of management to determine that they were in place and current.	No Exceptions Noted.
	Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected screen prints of the ticketing application and conducted a corroborative inquiry of management to determine that the tickets were created, worked, and documented as described.	No Exceptions Noted.
	Escalation procedures are in place to assign tickets to technical or application personnel that required an elevated level of support.	Inspected the Escalation and Standard Procedures Policy as contained within the Security Policies document and conducted a corroborative inquiry of management to determine that tickets followed escalation procedures when required by the nature of the issue.	No Exceptions Noted.

Trust Services Principle – Common Criteria (Continued)
Common Criteria to Security and Availabilty

CC7.0	Common Criteria Related to Change Management (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's Security and Availabilty commitments and system requirements.		
	Vulnerability assessments are performed by IT staff periodically to test for known vulnerabilities on the network and production systems.	Inspected sample scan results and conducted a corroborative inquiry of management to determine the assessments were performed as described.	No Exceptions Noted.
	An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems.	Inspected the Change Management Policy and Procedures as contained within the Security Policies and conducted a corroborative inquiry of management to determine that change was managed throughout the organization as described.	No Exceptions Noted.
	The Change review board or IT Management must approve proposed changes that affect the production environment.	For selected sample of infrastructure change tickets, inspected the ticket approval and conducted a corroborative inquiry of management to determine that changes were properly reviewed and approved.	No Exceptions Noted.
	Changes are authorized and scheduled when testing is complete.	For selected sample of change tickets, inspected the change process and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted.

Trust Services Principle – Availability

The system is available to users as committed or agreed

A1.0	Additional criteria related to availability		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.		
	The Company has a risk management program to address security and business-related risks.	Inspected the Risk Analysis Worksheet, risk topics as contained within the Security Policies. Risk review ticket and conducted inquiry of management to determine that the Company had a risk management program to address security and business-related risks.	No Exceptions Noted.
	A monitoring application is utilized to monitor network devices and critical systems.	Inspected screen prints of the monitoring applications and conducted inquiry of management to determine that the organization utilized monitoring applications to measure production systems utilization and availability.	No Exceptions Noted.
	A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices.	Inspected sample alerts and conducted inquiry of management to determine that sufficient notification takes place when predefined thresholds are exceeded.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.

Trust Services Principle – Availability
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.		
	A third party application is used to monitor network device Syslog and generate e-mail notifications when certain events occur. Logs are analyzed either manually or by automated tools to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.	Inspected sample automated alerts and conducted a corroborative inquiry of management to determine that the third party application generated notifications when certain network device events occurred.	No Exceptions Noted.
	Incoming Support tickets are prioritized based on the level of criticality and addressed by highest impacting request to ensure minimal disruption of service to users.	For selected sample of support tickets, inspected the support ticket priority and conducted a corroborative inquiry of management to determine that tickets were prioritized based on level of criticality and addressed by highest impacting request to minimize disruption of services.	No Exceptions Noted.

Trust Services Principle – Availability (Continued)
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.		
	The data center is equipped with water detection devices to prevent water damage in the event of a flood and/or water leak.	Observed the water detection systems to determine that the data center was equipped with water detection devices to prevent water damage in the event of a flood and/or water leak.	No Exceptions Noted.
	Personnel are on duty at the data center facility.	Inspected the NOC personnel schedule, observed the onsite personnel and conducted inquiry of management to determine that personnel were on duty at the data center facility.	No Exceptions Noted.
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected screen prints of the backup application and conducted inquiry of management to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted.
	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected screen prints of the automated backup notification settings, sample email notifications and conducted a corroborative inquiry of management to determine that computer operations personnel monitored the success or failure of data backups on a daily basis and were notified of backup job status via backup log entries and e-mail notifications.	No Exceptions Noted.
	Restores from backups can be performed to verify that system components can be recovered from backup media.	Inspected screen prints of the restore tests to determine that restores from backups can be performed to verify that system components can be recovered from backup media.	No Exceptions Noted.

Trust Services Principle – Availability (Continued)
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.		
	Backup media is transported to the alternate data center by Alchemy staff.	Inspected the media transfer logs and conducted inquiry of management to determine that backup media was transported to the alternate data center by Alchemy staff.	No Exceptions Noted.
	The Company has a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	Inspected the Incident Response Policy as contained within the Security Policies document and conducted inquiry of management to determine that the Company had a Security Incident Response Policy and Procedures in place to provide policy guidance for responding to and reporting security breaches.	No Exceptions Noted.
	The firewall is configured to generate e-mail notifications when certain firewall events occur.	Inspected screen prints of the firewall settings and conducted a corroborative inquiry of management to determine that it was configured to send notifications to administrators when certain events occurred.	No Exceptions Noted.
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Disaster Recovery & Business Continuity Plan and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted.
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the plan revision date and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted.

Trust Services Principle – Availability (Continued)
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.		
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the DR test ticket and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted.
	Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected screen prints of the ticketing application and conducted a corroborative inquiry of management to determine that the tickets were created, worked, and documented as described.	No Exceptions Noted.

Trust Services Principle – Availability (Continued)
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor's Test of Controls**	**Test Results**
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.		
	The Company cross trains employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	Inspected the employee roles listing the individuals trained to perform the job function and conducted corroborative inquiry of management to determine that the Company cross trained employees to perform multiple jobs, tasks, and functions for the purposes of business continuity.	No Exceptions Noted.
	Automated backup systems are utilized to perform the scheduled system backups of target data.	Inspected screen prints of the backup application and conducted inquiry of management to determine that an automated backup system was utilized to perform the scheduled system backups.	No Exceptions Noted.
	An inventory of backup media is maintained.	Inspected the backup media report and conducted a corroborative inquiry of management to determine that an inventory of backup media was maintained.	No Exceptions Noted.
	Backup media is physically secured while onsite and access is restricted to only authorized personnel.	Observed the secure media during onsite procedures to determine that backup media was secured while on-site and access was restricted to authorized personnel.	No Exceptions Noted.
	Restores from backups can be performed to verify that system components can be recovered from backup media.	Inspected screen prints of the restore tests to determine that restores from backups can be performed to verify that system components can be recovered from backup media.	No Exceptions Noted.

Trust Services Principle – Availability (Continued)
The system is available to users as committed or agreed

A1.0	Additional criteria related to availability (Continued)		
TSP	**Description of Controls In Place**	**Service Auditor’s Test of Controls**	**Test Results**
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.		
	Tape transfer logs are maintained to document the transfer of backup media to the alternate data center.	For selected sample of months, inspected the Offsite Tape Transfer Form and conducted inquiry of management to determine that management maintained media transfer logs tracking the media transported to the alternate data centers.	No Exceptions Noted.
	The Company has implemented countermeasures to protect against denial of service attacks.	Inspected the Denial Of Service Attack Procedure as contained within Security Policies to determine that the countermeasures to protect against DDOS attacks were in place.	No Exceptions Noted.
	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations.	Inspected the Disaster Recovery & Business Continuity Plan and conducted a corroborative inquiry of management to determine that it was in place to facilitate disaster recovery operations.	No Exceptions Noted.
	The disaster recovery plan is reviewed by management on an annual basis and revised as necessary.	Inspected the plan revision date and conducted a corroborative inquiry of management to determine that it was revised annually.	No Exceptions Noted.
	Certain aspects of the disaster recovery plan are tested on an annual basis.	Inspected the DR test ticket and conducted a corroborative inquiry of management to determine that certain aspects of the disaster recovery plan were tested within the last 12 months.	No Exceptions Noted.
	Changes are authorized and scheduled when testing is complete.	For selected sample of change tickets, inspected the change process and conducted a corroborative inquiry of management to determine that changes were authorized and scheduled when testing was complete.	No Exceptions Noted.

Assure conducted tests of the operating effectiveness of controls implemented by Alchemy Communications, Inc. Listed in the table below are all the noted exceptions.

Exceptions Noted

Description of Controls in Place	Service Auditor’s Test of Controls
Visitors must sign in and provide a government issued ID prior to issuance of a visitors badge. Visitors badges are for identification only and do not permit access to the facilities.	Observed the visitors check-in proces during onsite procedures to determine that visitors were required to sign the visitor log and were issued a visitor badge which was displayed by the visitor while on the premises.
Badge printer not connected as a result of remodeling during onsite walkthrough procedures at the LAX data center.	