Steadfast Networks
Type 2 SOC 2
2018

REPORT ON STEADFAST NETWORKS' DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

November 1, 2017 Through October 31, 2018

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT STEADFAST NETWORKS RELEVANT TO SECURITY AND AVAILABILITY

To Steadfast Networks:

We have examined the attached description titled "Description of Steadfast Networks' Colocation, Managed Services, and Cloud Services System Throughout the Period November 1, 2017 Through October 31, 2018" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period November 1, 2017 through October 31, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Steadfast Networks' ('Steadfast' or 'the Company') 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.

Steadfast uses Digital Capital Partners and Digital Realty Trust, Inc. ("subservice organizations") for colocation services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed and operating effectively. The description presents Steadfast's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations.

Steadfast has provided the attached assertion titled "Management of Steadfast Networks' Assertion Regarding Its Colocation, Managed Services, and Cloud Services System Throughout the Period November 1, 2017 Through October 31, 2018," which is based on the criteria identified in management's assertion. Steadfast is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Steadfast's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. 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, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period November 1, 2017 through October 31, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria 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. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in Steadfast's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period November 1, 2017 through October 31, 2018.
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 1, 2017 through October 31, 2018, and user entities applied the complementary user-entity controls contemplated in the design of Steadfast's controls throughout the period November 1, 2017 through October 31, 2018 and the subservice organization applied, throughout the period November 1, 2017 through October 31, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.
c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, and together with the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period November 1, 2017 through October 31, 2018.

The specific controls we tested, and the nature, timing, and results of our tests are presented in the section of our report titled "Information Provided by the Service Auditor".

This report and the description of tests of controls and results thereof are intended solely for the information and use of Steadfast; user entities of Steadfast's Colocation, Managed Services, and Cloud Services System during some or all throughout the period November 1, 2017 through October 31, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

A-LIGN ASSURANCE

November 19, 2018
Tampa, Florida

SECTION 2

MANAGEMENT OF STEADFAST NETWORKS' ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2017 THROUGH OCTOBER 31, 2018

Management of Steadfast Networks' Assertion Regarding Its System Throughout the Period November 1, 2017 through October 31, 2018

November 19, 2018

We have prepared the attached description titled "Description of Steadfast Networks' Colocation, Managed Services, and Cloud Services System Throughout the Period November 1, 2017 Through October 31, 2018" (the description), 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 1.34-.35 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 Colocation, Managed Services, and Cloud Services System, particularly system controls intended to meet the criteria for the Security and Availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (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 Colocation, Managed Services, and Cloud Services System throughout the period November 1, 2017 through October 31, 2018, 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 structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
      - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
      - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
      - *Processes*. The automated and manual procedures.
      - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

      (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 or other parties.

      (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (7) 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 service organization's system.

      (8) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

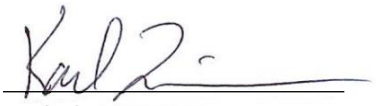
(9) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization'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 description were suitably designed throughout the specified period to meet the applicable trust services criteria.

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



Karl Zimmerman
CEO
Steadfast Networks

SECTION 3

DESCRIPTION OF STEADFAST NETWORKS' SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2017 THROUGH OCTOBER 31, 2018

OVERVIEW OF OPERATIONS

Company Background

Steadfast Networks, LLC is a privately held company that was founded in 1998 and registered in the state of Delaware in 2014. Steadfast is a cloud services firm that focuses on being the IT experts for mid-market businesses by providing flexible, well-designed, managed IT infrastructure solutions, including: public cloud, private cloud, hybrid cloud, dedicated servers, colocation, security, and network services. The Steadfast Networks data centers are engineered to provide mission-critical levels of performance and have delivered with 100% power uptime for dual corded devices for more than five years. Steadfast Networks' primary data centers are located in Chicago, Illinois.

Description of Services Provided

Cloud Services

The Steadfast Cloud Platform consists of a Storage Area Network (SAN) and a group of hypervisor machines that connect to the SAN. The SAN provides the necessary hard drive storage for each virtual machine. The hypervisors provide processing power and RAM. Each virtual machine uses resources provided by the SAN and the hypervisors.

The Steadfast Cloud Platform services allow customers to have completely isolated operating system installations on Steadfast Networks' shared hardware. It is based on Xen Hypervisor software managed by the OnApp software platform. Having an isolated operating system on secure, shared hardware allows optimal availability and utilization of resources. The resources of each virtual machine are instantly scalable through the cloud platform.

The Steadfast Cloud Platform is powered by high availability NetApp and Nimble Storage SANs. NetApp and Nimble Storage SANs are true enterprise hardware used by major corporations to withstand a full array of failures, with no single point of failure. 15,000 rpm Serial Attached SCSI (SAS) drives are used for primary storage with 1 TB of solid state cache. Serial Advanced Technology Attachment (SATA) storage is provided as an alternative to SAS drives.

The following list comprises offerings from the Steadfast Cloud Platform:

- High Availability
- Instant Deployment
- Hourly Billing
- Support
- VLAN Support
- Managed Services
- Tiered Storage
- Backup Management
- Console Access

High Availability

The Steadfast Cloud Platform is powered by fully redundant Cisco network infrastructure and redundant Supermicro servers. Redundancy allows for the failure of a switch with no reduction in maintaining 100% availability. If a physical hypervisor, to which the customer's virtual machine is assigned, fails, the customer's virtual machine is instantly deployed on another physical hypervisor with a minimal amount of down time.

Instant Deployment

Virtual machines are provided through on-demand public cloud servers with compute, storage, and bandwidth resources that can be deployed on-demand, in seconds, via an intuitive cloud dashboard, mobile app, and comprehensive API.

Hourly Billing

All resources are billed hourly and can be added or removed from a customer's account instantly at any time.

Support

Support is offered by the Steadfast Networks staff 24x7x365 via email and phone. All staff is in-house and on-site at the Steadfast Networks data centers.

VLAN Support

While Steadfast Networks' internal network is available for use for customers of the Steadfast Cloud Platform, virtual local area network (VLAN) support is also offered. Private VLANs allow customers to build a highly secure environment, with the option to connect to existing dedicated servers or colocation configurations.

Managed Services

All Steadfast Cloud Platform services come with managed services, including full operating systems and control panel software. In addition to OSs and control panels, software support and firewall support and setup are offered to customers as part of the overall Cloud Platform services offered.

Tiered Storage

In addition to SAS storage offered to customers, Serial Advanced Technology Attachment (SATA) storage is provided as an alternative. SATA storage is a cheaper solution that is optimal for archived data, infrequently accessed data, and backups. The backup of data on drives/subsystems separate from the local data allows for added security.

Backup Management

The Steadfast Cloud Platform allows the creation of backups. The option to schedule backups at set intervals is also available. Backups may be saved as images to be used to deploy new virtual machines.

Console Access

All virtual machines within the Steadfast Cloud Platform allow full virtual network computing (VNC) access.

Colocation

Colocation enables customers to lease controlled space in the data center to locate network, servers, SAN storage, and related customer equipment. Colocation is available in secure space increments including single rack units, ½ cabinet, full cabinet, and caged suites. Physical security includes visual confirmation and strict sign-in procedures, along with key cards, biometric scanning, and photo ID verification to ensure that only authorized personnel have access to the data center.

All data center sites follow the strict redundancy, security, and environmental standards and are backed by a 24x7x365 on-site staff and 100% power uptime SLA. Every location is also carrier neutral, providing customers with access to dozens of other carriers and networks. Colocation customers can also subscribe to Internet bandwidth services delivered via the Steadfast Networks meshed network. Customer networks are monitored for uptime and use on a 24x7x365 basis.

Available Locations:

- Chicago, Illinois (two locations)

Available Colocation Options:

- Single Server Rack
- Half cabinet
- Full cabinet
- Private Caged Space

Colocation Services Include:

- Premium IP Bandwidth (95th percentile, capped, or per GB billing options)
- Web-based Customer Portal for Support, Billing, Remote Boot, and Statistics
- Real-time Bandwidth Utilization Graphs
- Remote Boot and Power-down
- 24x7x365 Telephone and Ticketing Support
- Fully redundant network
- Dozens of Direct Peering partners
- FastE, Gigabit, or 10 Gigabit Ports

Managed Dedicated Servers

Dedicated servers are servers that the company provides to customers for a monthly fee. The entire server, including all hardware, is restricted and committed to an individual customer. This service enables customers to utilize the benefits of having total control over servers without the upfront costs associated with purchasing servers and the recurring costs of continuing maintenance and inventory management associated with using colocation services. This service is most beneficial to customers who need full control over every aspect of a server. All private cloud and dedicated server packages feature a premium layer of all-inclusive managed services, referred to as the “Steadfast Advantage”.

“Steadfast Advantage” (Managed Services):

- 99.99% Availability SLA
- 1 Hour (or Less) Support Response SLA
- Migration Services
- OS Patching
- Trusted Advisor/Engineering
- Performance Diagnostics Report
- Advanced System & Networking Monitoring
- Proactive Response and Resolution of Monitoring
- Security Analysis & Ongoing Auditing

Steadfast Networks uses Digital Realty Trust, Inc., Digital Capital Partners, LLC, and IO Data Centers, LLC (“the Subservice Organizations”) for the physical storage including physical security controls and environmental safeguards of some of the racks hosting client equipment. This description does not include the control objectives and related controls of the Subservice Organizations.

Significant Events

Steadfast Networks has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Colocation, Managed Services, and Cloud Services systems. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Infrastructure

Primary infrastructure used to provide Steadfast Networks' Colocation, Managed Services, and Cloud Services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Juniper MX Series	Network	Core Routers
Juniper EX9200 Series	Network	Distribution Switches
Cisco 6500 Series	Network	Distribution Switches
Cisco 2960 Series	Network	Access Switches
Juniper EX Series	Network	Access Switches
Xeon Servers	Cloud	OnApp Cloud Hypervisors and CP Server
Xeon Servers	Infrastructure	Ubersmith CP and Appliance Servers
Xeon Servers	Infrastructure	Veeam and R1Soft Backup Servers
Xeon Hypervisors	Linux Infrastructure	KVM-based Utility and Core Application VMs
Xeon Hypervisors	Windows Infrastructure	Hyper-V-based Utility and Core Application VMs
Mixed Server Hardware	Infrastructure	DNS and Provisioning Services
Mixed Server Hardware	Infrastructure	Additional Core Applications

Software

Primary software used to provide Steadfast Networks' Colocation, Managed Services, and Cloud Services system includes the following:

Primary Software	
Software	**Purpose**
OnApp	Cloud Management Software Solution
Ubersmith	Billing Software and Data Center Management
Kayako Fusion	Support Ticketing System
R1Soft Server Backup	Data Backup
Veeam	Data Backup

People

The Steadfast Networks staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Processes

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Steadfast policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Steadfast team member.

Physical Security

Wholly occupied company facilities are protected by walls around the entire perimeter. Each facility has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day. Access to the reception area is unlocked from 8am to 5pm on business days and is locked at all other times. When locked, a visitor presses a buzzer to attract the attention of the guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by a Steadfast employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Upon an employee's termination of employment, HR sends an access removal request on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview.

Logical Access

Steadfast uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Steadfast implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Steadfast network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees' access Colocation, Managed, and Cloud services through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Steadfast's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. In the days leading up to the start date of the new employee, an Access Authorization form is completed which outlines the required systems and access for the position.

On an annual basis, access rules for each role are reviewed by management. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CTO and COO. As part of this process, the CTO and COO review access by privileged roles and requests modifications based on this review.

In conjunction with employee termination, HR initiates steps to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

Contracted customer off-site tape rotations are logged and maintained within an enterprise ticket management system. A third-party provider that specializes in off-site tape rotation has been contracted to perform off-site tape rotation services for clients that select this as part of the backup service. The ability to recall backup media from the third-party off-site storage facility is restricted to authorized operations personnel.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Steadfast monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Steadfast evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

Steadfast has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Steadfast system owners review proposed operating system patches to determine whether the patches are applied. Customers and Steadfast systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Steadfast staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Steadfast maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Steadfast has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Steadfast system owners review proposed operating system patches to determine whether the patches are applied. Customers and Steadfast systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Steadfast staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Steadfast. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Steadfast policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Steadfast. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Steadfast system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Steadfast in delivering its Colocation, Managed, and Cloud services system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Boundaries of the System

The scope of this report includes the Colocation, Managed Services, and Cloud Services system performed in the Chicago, Illinois facility.

Subservice Organizations

This report does not include the colocation services provided by Digital Capital partners at the Chicago, Illinois facility or Digital Realty Trust, Inc. at the Chicago Illinois facility.

Significant Events and Conditions

Steadfast has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Colocation, Managed, and Cloud services system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

Steadfast utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Subservice Organizations

The colocation services provided by Digital Realty Trust, Inc. and Digital Capital Partners are monitored by management and have not been included in the scope of this review. The following criteria and controls are implemented by Digital Realty Trust, Inc. and Digital Capital Partners.

Subservice Organization Controls - Digital Capital Partners and Digital Realty Trust, Inc.		
Principle	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC5.5	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Data centers are protected by fire detection and suppression systems.
		Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure.
		Data centers have generators to provide backup power in case of electrical failure.

Criteria Not Applicable to the System

All Common and Availability criteria were applicable to the Steadfast Colocation, Managed, and Cloud services system.

Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Steadfast's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Steadfast's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

Steadfast's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Steadfast's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Steadfast's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Steadfast's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

Steadfast's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Steadfast's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

Steadfast's risk assessment process identifies and manages risks that could potentially affect Steadfast's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Steadfast identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Steadfast, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Steadfast has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Steadfast attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

TRUST SERVICES PRINCIPLES AND CRITERIA

Although the trust services criteria and related controls are presented in section 4, "Information Provided by the Service Auditor," they are an integral part of Steadfast's system description.

In-Scope Trust Services Principles

Common Criteria (to the Security and Availability Principles)
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

Availability
The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems) but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Steadfast's Colocation, Managed, and Cloud services system; as well as the nature of the components of the system result in risks that the criteria will not be met. Steadfast addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Steadfast's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Steadfast's description of the system. Any applicable trust services criteria that are not addressed by control activities at Steadfast are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Steadfast's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Steadfast's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Steadfast's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Steadfast's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication is an integral component of Steadfast's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Steadfast, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, meetings are held to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Steadfast personnel via e-mail messages.

Specific information systems used to support Steadfast's Colocation, Managed, and Cloud services system are described in the Description of Services section above.

COMPLEMENTARY USER ENTITY CONTROLS

Steadfast's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to Steadfast's services to be solely achieved by Steadfast control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Steadfast.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for communicating to Steadfast Networks a list of personnel authorized to access the facilities and periodically reviewing and updating this list in the customer portal.
2. User entities are responsible for using the customer portal to maintain up to date user information and access credentials around core Steadfast Networks services.
3. User entities are responsible for using strong password and access codes to access all systems, including, but not limited to the customer portal, servers, and applications on the servers.
4. User entities are responsible for responding to critical event notifications from Steadfast Networks.
5. User entities are responsible for complying with all laws and regulations with respect to security, availability, maintainability, and integrity.
6. User entities are responsible for appropriate design and implementation of security architecture for customer equipment including firewalls, switch, and router configuration.
7. User entities are responsible for restricting access to customer infrastructure, hardware, networks, operating systems, applications databases, and any other systems located or accessible using Steadfast Networks bandwidth.
8. User entities are responsible for having authorized personnel available to report issues and discuss them with Steadfast Networks personnel.
9. User entities are responsible for notifying Steadfast Networks via the customer portal or ticketing system with any changes or updates to their notification information.
10. User entities are responsible for working with Steadfast Networks to resolve operational problems.
11. User entities are responsible for technical support for customer equipment at Steadfast Networks and to their end users.
12. User entities are responsible for configuring, administering, monitoring, and repairing all customer software and hardware failures.
13. User entities are responsible for understanding and complying with the terms of service and their contractual obligations to Steadfast Networks.
14. User entities are responsible for immediately notifying Steadfast Networks of any actual or suspected information security breaches, including compromised user accounts.
15. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Steadfast Networks' services.
16. User entities are responsible for notifying Steadfast Networks of on-site visits of employees, vendors, and contractors prior to arrival at the data center.
17. User entities are responsible for ensuring the security of any keys or badges used to access Steadfast Networks facilities.
18. User entities are responsible for ensuring their cabinets are locked and their equipment is secured prior to leaving the premises, when applicable.
19. User entities are responsible for providing insurance for their hardware, software, data and other equipment.
20. User entities are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.
21. User entities are responsible for implementing a security infrastructure and practices to prevent unauthorized access to their internal network and limit threats from connections to external networks.
22. User entities are responsible for maintaining local copies of their content and other stored information, including backups.
23. User entities are responsible for the integrity of all backups.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Steadfast was limited to the Trust Services Principles and related criteria and control activities specified by the management of Steadfast and did not encompass all aspects of Steadfast's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
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 availability.	Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and are evaluated as part of the hiring or transfer evaluation process.	Inspected a sample of job descriptions to determine that job requirements were documented in the job descriptions and were evaluated as part of the hiring or transfer evaluation process.	No exceptions noted.
		The experience of candidates for employment of transfer are evaluated as a component of the hiring process.	Inspected the hiring procedures to determine that the experience of candidates for employment of transfer were evaluated as a component of the hiring process.	No exceptions noted.
		Periodic training is completed at least annually by personnel related to the security and availability of products.	Inquired of the Chief Financial Officer regarding the training completion to determine that periodic training was completed at least annually by personnel related to the security and availability of products.	No exceptions noted.
			Inspected the security awareness training log for a sample of current employees to determine that periodic training was completed at least annually by personnel related to the security and availability of products.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability.	Personnel are required to read and accept the code of conduct upon hire.	Inspected the signed code of conduct for a sample of new hires to determine that personnel were required to sign and accept the code of conduct upon hire.	No exceptions noted.
		Job requirements are documented in the job descriptions in the company WIki and candidates' abilities to meet these requirements are evaluated as part of the hiring evaluation process.	Inspected the company Wiki to determine that job requirements were documented in the job descriptions in the company Wiki and candidates' abilities to meet these requirements were evaluated as part of the hiring evaluation process.	No exceptions noted.
		Personnel are required to pass a background check provided by a third-party vendor upon hire.	Inspected the completed background check results for a sample of new hires to determine that personnel were required to pass a background check provided by a third-party vendor upon hire.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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.	System descriptions are communicated to authorized external users via service level agreements that delineate the boundaries of the system and describe relevant system components.	Inspected the external system description and a sample of new client SLA's to determine that system descriptions were communicated to authorized external users via service level agreements that delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		A description of the system is posted on a secure network drive and is available to personnel. This description delineates the boundaries of the system and key aspects of the monitoring services.	Inspected the steadfast wiki to determine that a description of the system was posted on a secure network drive and was available to personnel. This description delineates the boundaries of the system and key aspects of the monitoring services.	No exceptions noted.
CC2.2	The entity's security and availability 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 entity's security and availability commitments regarding the system are included in the master services agreement and customer specific service level agreements.	Inspected service level agreements for a sample of new customers to determine that the entity's security and availability commitments regarding the system were included in the master services agreement and customer specific service level agreements.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security policies and procedures to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to read and accept the code of conduct upon hire.	Inspected the signed code of conduct for a sample of new hires to determine that personnel were required to sign and accept the code of conduct upon hire.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected a sample of service level agreements to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedures documents for significant processes that address system requirements are available on the intranet.	Inspected the security policies and procedures to determine that policy and procedure documents for significant processes were available on the entity's intranet.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected a sample of service level agreements to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
		The entity's security and availability commitments regarding the system are included in the master services agreement and customer specific service level agreements.	Inspected service level agreements for a sample of new customers to determine that the entity's security and availability commitments regarding the system were included in the master services agreement and customer specific service level agreements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	Policy and procedures documents for significant processes are available on the intranet.	Inspected the security policies and procedures to determine that policy and procedures documents for significant processes were available on the intranet.	No exceptions noted.
		Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	Inspected a sample of service level agreements to determine that processes were monitored through service level management procedures to help ensure compliance with service level commitments and agreements.	No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security policies and procedures to determine that policy and procedures documents for significant processes were available on the intranet.	No exceptions noted.
		The entity's security and availability commitments regarding the system are included in the master services agreement and customer specific service level agreements.	Inspected service level agreements for a sample of new customers to determine that the entity's security and availability commitments regarding the system were included in the master services agreement and customer specific service level agreements.	No exceptions noted.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	All system changes are initiated and approved by management prior to changes being made in production.	Inspected a sample of change tickets to determine that all system changes were initiated and approved by management prior to changes being made in production.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Emergency changes are reviewed and approved by management post implementation.	Inspected a sample of high severity tickets and determined that emergency changes were reviewed and approved by management post implementation.	No exceptions noted.
		Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal users via e-mail as part of the change management process.	Inspected an example communication to determine that major changes to roles and responsibilities and changes to key personnel were communicated to affected internal users via e-mail as part of the change management process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system security and availability 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.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	Inspected the most recent risk assessment report to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	Inspected the most recent risk assessment report to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 entity has a formal risk management process that specifies management's evaluation of the implementation and effectiveness of controls defined regarding security and confidentiality.	Inspected the most recent risk assessment report to determine that the entity had a formal risk management process that specified management's evaluation of the implementation and effectiveness of controls defined regarding security and confidentiality.	No exceptions noted.
		Business recovery plans are tested periodically, but at least annually.	Inspected the business recovery plan to determine that business recovery plans were tested periodically, but at least annually.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent vulnerability scans to determine that vulnerability scans were performed at least annually, and their frequency was adjusted as required to meet ongoing and changing commitments and requirements.	No exceptions noted.
		During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	Inspected the most recent risk assessment report to determine during the risk assessment and management process, management personnel identified changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		During the risk assessment and management process, risk management office personnel identify environmental, regulatory, and technological changes that have occurred.	Inspected the most recent risk assessment report to determine during the risk assessment and management process, management personnel identified environmental, regulatory, and technological changes that have occurred.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	**Common Criteria Related to Monitoring of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected an example monitoring alert and the monitoring configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inspected the security and availability policy and procedures to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent vulnerability scans to determine that vulnerability scans were performed at least annually, and their frequency was adjusted as required to meet ongoing and changing commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability.	Documented policies and procedures are in place for system authentication, access, and security monitoring.	Inspected the information security policy manual to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Assets are assigned owners who are responsible for evaluating access based on job roles.	Inspected the network administrator list and list of system components to determine that assets were assigned owners who were responsible for evaluating the appropriateness of access based on job roles.	No exceptions noted.
		Online applications match each user ID to a single customer account number.	Inspected application login authentication to determine that the online application matched each user ID to a single customer account number.	No exceptions noted.
		External access by employees is permitted only through a two factor encrypted virtual private network (VPN) connection.	Inspected the VPN configuration to determine that external access by employees was permitted only through a two factor encrypted virtual private network (VPN) connection.	No exceptions noted.
		A role based security process has been defined with an access control system that is required to use roles when possible.	Inspected the user access list to determine that a role based security process had been defined with an access control system that was required to use roles when possible.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles.	Inspected the master list of system components to determine that assets were assigned owners who were responsible for evaluating the appropriateness of access based on job roles.	No exceptions noted.
		For software or infrastructure that does not support the use of role- based security, a separate database of roles and related access is maintained.	Inspected the user list with assigned access levels to determine that for software or infrastructure that does not support the use of role- based security, a separate database of roles and related access was maintained.	No exceptions noted.
		Privileged access to sensitive resources is restricted to defined user roles.	Inspected access control lists to determine that privileged access to sensitive resources was restricted to defined user roles.	No exceptions noted.
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 availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures were in place regarding user access authorization, provisioning, and revocation.	Inspected the information security policy to determine that documented policies and procedures were in place regarding user access authorization, provisioning, and revocation.	No exceptions noted.
		Standardized user access request forms are utilized to request access to the production system.	Inspected the user access request forms for a sample of new hires to determine that standardized user access request forms were utilized to request access to the production system.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access removal tickets are created and processed upon termination of an employee.	Inspected the user access list and a sample of access removal forms for terminated employees to determine that access removal tickets were created and processed upon termination of an employee.	No exceptions noted.
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 availability.	Documented policies and procedures are in place for system authentication, access, and security monitoring.	Inspected the information security policy manual to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		The online application matches each user ID to a single customer account number.	Inspected application login authentication to determine that the online application matched each user ID to a single customer account number.	No exceptions noted.
		Encrypted VPN channels help to ensure that only valid users gain access to IT components.	Inspected the VPN configuration to determine encrypted VPN channels helped to ensure that only valid users gain access to IT components.	No exceptions noted.
		Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.	Inspected the remote access policy to determine that users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Password complexity standards are established to enforce control over access control software passwords.	Inspected the information security policy and authentication to determine that password complexity standards were established to enforce control over access control software passwords.	No exceptions noted.
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 availability.	A role based security process has been defined with an access control system that is required to use roles when possible.	Inspected the user access list to determine that a role based security process had been defined with an access control system that was required to use roles when possible.	No exceptions noted.
		Standardized user access request forms are utilized to request access to the production system.	Inspected the user access request tickets for a sample of new hires to determine that standardized user access request forms were utilized to request access to the production system.	No exceptions noted.
		Logical access control self-assessment reviews are performed on an annual basis.	Inspected the most recent annual logical access review to determine that logical access control self-assessment reviews were performed on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability.	A badge access system is in place to restrict access to authorized personnel.	Inspected the badge access list to determine that a badge access system was in place to restrict access to authorized personnel.	No exceptions noted.
		Permissioned physical access is granted as part of the new hire onboarding process.	Inspected a sample of new hire access checklists to determine that permissioned physical access was granted as part of the new hire onboarding process.	No exceptions noted.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.	Observed the visitor procedure to determine that all visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components were maintained and operated.	No exceptions noted.
			Inspected the physical security policy to determine that all visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.	No exceptions noted.
		Physical access control self-assessment reviews are performed on an annual basis.	Inspected the integrity check results to determine that physical access control self-assessment reviews were performed on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Owners of sensitive areas of the facilities review access to their areas on an-annual basis.	Inspected the integrity check results to determine that owners of sensitive areas of the facilities reviewed access to their areas on an annual basis.	No exceptions noted.
		Physical access credentials are returned upon termination of an employee.	Inspected a sample of completed termination tickets to determine that physical access credentials were returned upon termination of an employee.	No exceptions noted.
		The sharing of access badges and tailgating are prohibited by policy.	Inspected the physical security policy to determine that the sharing of access badges and tailgating were prohibited by company policy.	No exceptions noted.
		A badge access system is in place to restrict access to authorized personnel.	Inspected the badge access list to determine that a badge access system was in place to restrict access to authorized personnel.	No exceptions noted.
		Please refer to the Subservice Organizations section above for additional controls managed by the subservice organization.	Not applicable.	Not applicable.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Documented policies and procedures are in place for system authentication, access, and security monitoring.	Inspected the information security policy manual to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A redundant firewall system is in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	Inspected the network diagram and firewall ruleset to determine that a redundant firewall system was in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	No exceptions noted.
		External access to nonpublic sites is restricted through the use of user authentication and message encryption systems such as VPN and SSL.	Inspected the network diagram and firewall ruleset to determine that external access to nonpublic sites was restricted through the use of user authentication and message encryption systems such as VPN and SSL.	No exceptions noted.
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 availability.	Encryption technologies are used for defined points of connectivity.	Inspected the encryption policy, encryption configuration, and firewall ruleset to determine that encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the encryption policy, to determine entity's policies prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
		Backup media are encrypted during creation.	Inspected the encryption policy and configuration to determine that backup media was encrypted during creation.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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 availability.	Antivirus software is installed on production servers and workstations.	Inspected the antivirus software configuration to determine that antivirus software was installed on production servers and workstations.	No exceptions noted.
		Antivirus software is updated automatically as new updates become available.	Inspected the antivirus update configuration to determine that antivirus software was updated automatically as new updates become available.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent vulnerability scans to determine that vulnerability scans were performed at least annually, and their frequency was adjusted as required to meet ongoing and changing commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	Vulnerabilities of system components to security and availability 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 availability.	Logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	Inspected an example monitoring alert and the monitoring configurations to determine that logging and monitoring software was used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Daily backups are performed using an automated system.	Inspected the backup system configuration and schedule to determine that backups were performed using an automated system.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent vulnerability scans to determine that vulnerability scans were performed at least annually, and their frequency was adjusted as required to meet ongoing and changing commitments and requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.2	Security and availability 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.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the incident response policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		The resolution of events is communicated to both internal and external users within the corresponding ticket.	Inspected a sample of problem tickets to determine that the resolution of events was communicated to both internal and external users within the corresponding ticket.	No exceptions noted.
		Change management requests are opened for events that require permanent fixes.	Inspected a sample of change tickets to determine that change management requests were opened for events that require permanent fixes.	No exceptions noted.
		The resolution of events is communicated to both internal and external users within the corresponding ticket.	Inspected a sample of problem tickets to determine that the resolution of events was communicated to both internal and external users within the corresponding ticket.	No exceptions noted.
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Inspected the employee handbook to determine that entity policies included probation, suspension, and termination as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	A documented policy is in place to guide personnel in the handling of system changes.	Inspected the ticket handling procedures to determine that a documented procedure was in place to guide personnel in the handling of system changes.	No exceptions noted.
		Changes are approved by management prior to implementation.	Inspected a sample of change tickets to determine that changes were approved by management prior to implementation.	No exceptions noted.
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 availability.	A formal risk assessment is performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	Inspected the risk assessment performed to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security and availability commitments and requirements.	No exceptions noted.
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 availability.	A root cause analysis is prepared and reviewed by operations management for high severity incidents.	Inspected a sample of high severity incident tickets to determine that a root cause analysis was prepared and reviewed by operations management for high severity incidents.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	System changes are reviewed and approved by management prior to implementation.	Inspected a sample of change tickets to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are tested prior to implementation and the types of testing performed depend on the nature of the change.	Inspected a sample of change tickets to determine that system changes were tested prior to implementation and the types of testing performed depended on the nature of the change.	No exceptions noted.
		Documented policies and procedures are in place for system authentication, access, and security monitoring.	Inspected the information security policy manual to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the IT infrastructure and environment to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inspected a sample of changes to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		Changes are reviewed and approved by management prior to implementation.	Inspected a sample of change tickets to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Daily backups are performed for rollback capability in the event that a system change does not function as designed.	Inspected the backup system configuration and schedule to determine that daily backups were performed for rollback capability in the event that a system change does not function as designed.	No exceptions noted.
		Post implementation procedures that are designed to verify the operation of system changes are performed for one week after the implementation for other than minor changes, and results are shared with users and customers as required to meet commitments and requirements.	Inspected a sample of changes to determine that post implementation procedures that were designed to verify the operation of system changes were performed for one week after the implementation for other than minor changes, and results were shared with users and customers as required to meet commitments and requirements.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	Inspected the change management policy and procedure to determine that the change management process had defined the following roles and assignments: • Authorization of change requests-owner or business unit manager • Development-application design and support department • Testing-quality assurance department • Implementation software change management group	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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.	Enterprise monitoring software is utilized to notify personnel when predefined thresholds are exceeded on production systems.	Inspected the system monitoring software configuration and a sample of alert notifications to determine that enterprise monitoring software was utilized to notify personnel when predefined thresholds are exceeded on production systems.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the system monitoring logs to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
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.	Management has contracted with a third-party data center to provide secure hosting of production systems and data.	Inspected the service agreement with the third-party data centers to determine that management has contracted with a third-party data center to provide secure hosting of production systems and data.	No exceptions noted.
		Environmental protections have been installed by and are maintained by the third-party data centers including the following: • HVAC • UPS • Generator backups in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Fire suppression system	Inspected the service agreement with the third-party data centers to determine that environmental protections were installed and maintained by the third-party data centers including the following: • HVAC • UPS • Generator backups in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Fire suppression system	No exceptions noted.

A1.0	AVAILABILITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Weekly full-system and daily incremental backups are performed using an automated system.	Inspected the backup system configuration and schedule to determine that daily backups were performed using an automated system.	No exceptions noted.
		Backups are monitored for failure using an automated system and the incident management process is automatically invoked.	Inspected the backup notification configuration and example backup alerts to determine that backups are monitored for failure using an automated system and the incident management process is automatically invoked.	No exceptions noted.
		Business continuity and disaster recovery plans have been developed and updated annually.	Inspected the business continuity and disaster recovery plan to determine that business continuity and disaster recovery plans have been developed and updated annually.	No exceptions noted.
		The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	Inspected the business continuity and disaster recovery plan to determine that the entity used a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	No exceptions noted.
		Please refer to the Subservice Organizations section above for additional controls managed by the subservice organization.	Not applicable.	Not applicable.

A1.0	AVAILABILITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	Inspected the business continuity and disaster recovery plan to determine that the entity used a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.	No exceptions noted.
		Business continuity and disaster recovery plans, including restoration of backups, are tested annually. Test results are reviewed, and the plan is adjusted accordingly.	Inquired of the Chief Financial Officer regarding the review of test results to determine that business continuity and disaster recovery plans, including restoration of backups, were tested annually, and that test results were reviewed, and the plan was adjusted accordingly.	No exceptions noted.
			Inspected the disaster recovery plan and test results to determine that business continuity and disaster recovery plans, including restoration of backups, were tested annually, and that test results were reviewed, and the plan was adjusted accordingly.	No exceptions noted.