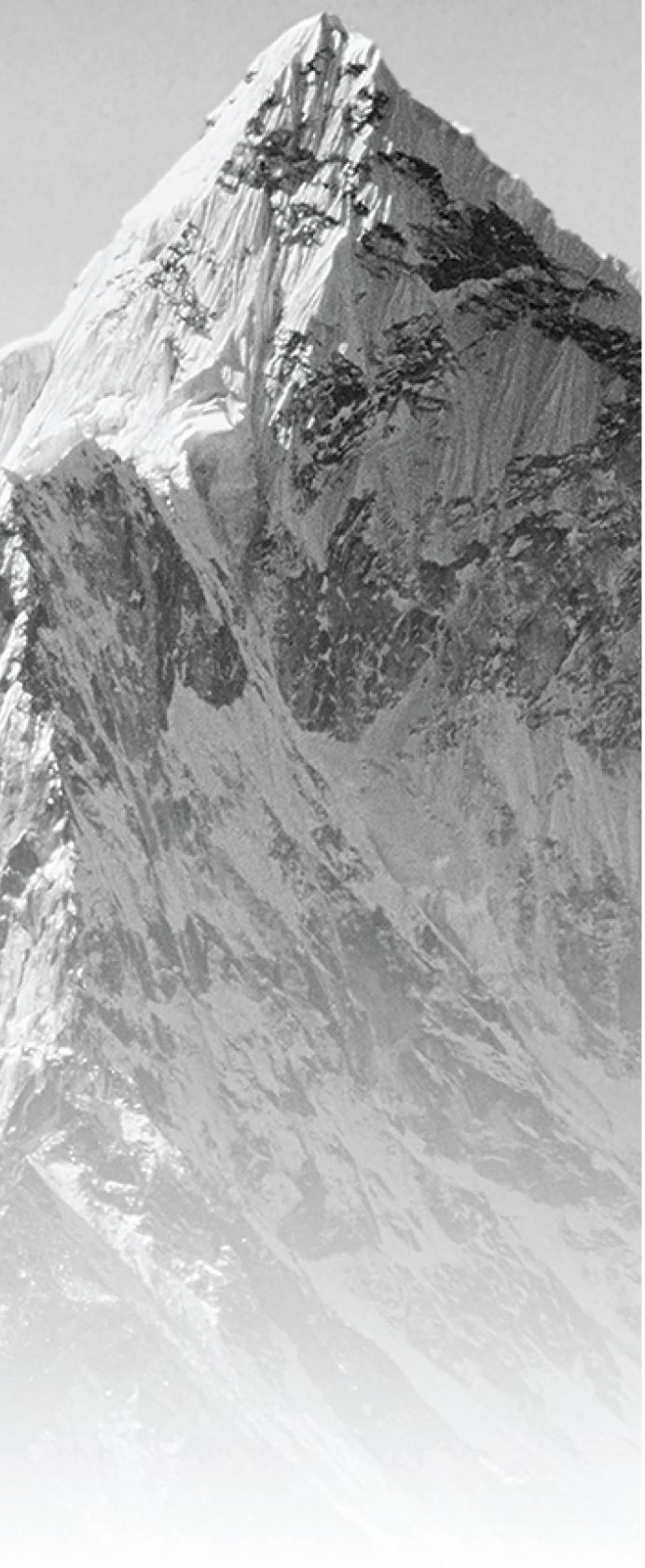


Steadfast Networks, LLC
Type 2 SOC 1
2018

REPORT ON MANAGEMENT'S DESCRIPTION OF STEADFAST NETWORKS, LLC'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2

November 1, 2017 Through October 31, 2018

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF STEADFAST NETWORKS, LLC'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

To Steadfast Networks, LLC:

We have examined Steadfast Networks, LLC's ('Steadfast' or 'the Company') description of its Colocation, Managed Services, and Cloud Services system at its Chicago, Illinois location for providing colocation, managed, and cloud services for the period November 1, 2017 through October 31, 2018, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description, based on the criteria identified in the "Steadfast Networks Assertion" (assertion). The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Steadfast's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and 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 in Section 3 includes only the controls and related control objectives of Steadfast and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Steadfast can be achieved only if complementary subservice organization controls assumed in the design of Steadfast are suitably designed and operating effectively, along with the related controls at Steadfast. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

In Section 2 of this report, Steadfast has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Steadfast is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, 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, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description for the period November 1, 2017 through October 31, 2018.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description.

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 achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in its Colocation, Managed Services, and Cloud Services system. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in Steadfast's assertion in Section 2 of this report,

- the description fairly presents the system that was designed and implemented for the period November 1, 2017 through October 31, 2018.
- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively for the period November 1, 2017 through October 31, 2018 and subservice organizations and user entities applied the complementary controls contemplated in the design of Steadfast's controls for the period November 1, 2017 through October 31, 2018.
- the controls tested, which together with the complementary subservice organization and user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively for the period November 1, 2017 through October 31, 2018.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Steadfast, user entities of Steadfast's system during some or all of the period November 1, 2017 through October 31, 2018, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

November 19, 2018
Tampa, Florida

SECTION 2

STEADFAST NETWORKS' ASSERTION

Steadfast Networks' Assertion

November 19, 2018

We have prepared the description of Steadfast Networks, LLC's Colocation, Managed Services, and Cloud Services system for providing colocation, managed, and cloud services during some or all of the period November 1, 2017 through October 31, 2018 (description) for user entities of the system during some or all of the period November 1, 2017 through October 31, 2018, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Steadfast uses subservice organizations for colocation services. The description includes only the control objectives and related controls of Steadfast and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Steadfast controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the Colocation, Managed Services, and Cloud Services system made available to user entities of the system during some or all of the period November 1, 2017 through October 31, 2018 for processing their transactions. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to provide colocation, managed, and cloud services, including:

      (1) The types of services provided.

      (2) The procedures, within both automated and manual systems, by which services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      (3) How the system captures significant events and conditions, other than transactions.

      (4) The process used to prepare reports and other information for user entities.

      (5) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

      (6) Other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. does not omit or distort information relevant to the scope of the Colocation, Managed Services, and Cloud Services system, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Colocation, Managed Services, and Cloud Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

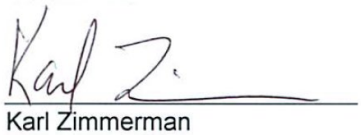
b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. The controls related to the control objectives stated in the description were suitably designed and operated effectively for the period November 1, 2017 through October 31, 2018 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Steadfast's controls throughout the period November 1, 2017 through October 31, 2018. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Karl Zimmerman
CEO
Steadfast Networks

SECTION 3

DESCRIPTION OF THE SYSTEM PROVIDED BY THE SERVICE ORGANIZATION

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. 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 a high availability NetApp SAN. The NetApp SAN is 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

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

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 directly from the control panel. 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

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 Server

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):

- 24/7 Phone & Email Support
- 100% Network & Power Uptime SLA
- 1 Hour (or Less) Support Response SLA
- 1 Hour (or Less) Hardware Replacement SLA
- OS Patching / Security Updates
- Advanced System & Networking Monitoring
- Proactive Response and Resolution of Monitoring
- Security Analysis & Ongoing Auditing

Steadfast Networks uses Digital Realty Trust, Inc. and Digital Capital Partners, 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.

Functional Areas of Operation

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

Boundaries of the System

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

Subservice Organizations

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

Subservice Organization Controls

Steadfast's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called subservice organization controls. It is not feasible for all the control objectives related to Steadfast's services to be solely achieved by Steadfast control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Steadfast. Digital Reality Trust, Inc. and Digital Capital Partners provide physical controls around the security of infrastructure at the data center housing facility.

The following subservice organization controls should be implemented by Digital Capital Partners to provide additional assurance that the control objectives described within this report are met:

Subservice Provider - Digital Capital Partners	
Control Objective	**Control**
Physical Security	Physical security of the data centers is controlled through limited access points
	Physical security of the suites is controlled through a badge and/or biometric reader
	Access to master keys is restricted to personnel from the Security, Engineering and Site Management teams
Environmental Security	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

Subservice Provider - Digital Capital Partners	
Control Objective	**Control**
	Data centers have generators to provide backup power in case of electrical failure
	The entity provides fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies

The following subservice organization controls should be implemented by Digital Realty Trust, Inc. to provide additional assurance that the control objectives described within this report are met:

Subservice Provider - Digital Realty Trust, Inc.	
Control Objective	**Control**
Physical Security	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
Environmental Security	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
	The entity provides fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies

Steadfast management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Steadfast performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Making regular site visits to vendor and subservice organization's facilities
- Reviewing applicable attestation reports over services provided by vendors and subservice organizations

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities on the 12 months preceding the end of the review period.

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 Networks' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Steadfast Networks' 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 Networks' 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 certain 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 Networks' 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 Networks' 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 Networks' 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 Networks' 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 Networks' 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 acknowledgment 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 Networks' risk assessment process identifies and manages risks that could potentially affect Steadfast Networks' 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 Networks 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 Networks, 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 Networks 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 Networks attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, Steadfast Networks has identified and put into effect actions needed to address those risks. To address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which Steadfast Networks strives to achieve its business objectives. Steadfast Networks has applied a risk management approach to the organization to select and develop control activities. After relevant risk have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

Steadfast Networks' control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of Steadfast Networks' description of the data center services system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. 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 Networks' 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 Networks' 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 Networks' 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 Networks' 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 Systems

Steadfast Networks has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable Steadfast Networks to understand business trends to maximize efforts and provide optimal services.

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

Primary Software	
Software	**Purpose**
Kayako Case	Support Ticketing System
R1Soft Server Backup	Data Backup
Veeam	Data Backup

Communication Systems

Communication is an integral component of Steadfast Networks' 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 Networks, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly meetings 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 Networks personnel via e-mail messages.

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 control objectives 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 control objectives 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.

Control Objective 1 - New Customer Setup and Maintenance

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 notifying Steadfast Networks via the customer portal or ticketing system with any changes or updates to their notification information.

Control Objective 2 - Customer Support - Business Problems

5. User entities are responsible for configuring, administering, monitoring, and repairing all customer software and hardware failures.

Control Objective 3 – Customer Support System Availability

6. User entities are responsible for responding to critical event notifications from Steadfast Networks.
7. User entities are responsible for complying with all laws and regulations with respect to security, availability, maintainability, and integrity.
8. User entities are responsible for appropriate design and implementation of security architecture for customer equipment including firewalls, switch, and router configuration.
9. 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.

Control Objective 4 - Information Security

10. 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.
11. User entities are responsible for having authorized personnel available to report issues and discuss them with Steadfast Networks personnel.
12. User entities are responsible for working with Steadfast Networks to resolve operational problems.
13. User entities are responsible for technical support for customer equipment at Steadfast Networks and to their end users.

Control Objective 6 - Computer Operations

14. User entities are responsible for understanding and complying with the terms of service and their contractual obligations to Steadfast Networks.
15. User entities are responsible for immediately notifying Steadfast Networks of any actual or suspected information security breaches, including compromised user accounts.
16. User entities are responsible for providing insurance for their hardware, software, data and other equipment.
17. User entities are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.
18. 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.
19. User entities are responsible for maintaining local copies of their content and other stored information, including backups.
20. User entities are responsible for the integrity of all backups.

SECTION 4

TESTING OF CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES 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 control objectives and related control activities specified by the management of Steadfast and did not encompass all aspects of Steadfast's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

Our examination of the control activities was 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 a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

CONTROL AREA 1 **New Customer Setup and Maintenance**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Steadfast maintains new customer setup and provisioning policies and procedures, which are reviewed by executive management on at least a semi-annual basis.	Inquired of the Chief Financial Officer regarding annual policy review to determine that Steadfast maintained new customer setup and provisioning policies and procedures, which were reviewed by executive management on at least a semi-annual basis.	No exceptions noted.
		Inspected the new customer setup and provisioning policies and procedures to determine that Steadfast maintained new customer setup and provisioning policies and procedures, which were reviewed by executive management on at least a semi-annual basis.	No exceptions noted.
1.2	Employees are required to familiarize themselves with the policies concerning customer setup and sign an acknowledgement of their understanding and willingness to comply with these policies and procedures.	Inspected the signed acknowledgement for a sample of new employees to determine that employees were required to familiarize themselves with the policies concerning customer setup and signed an acknowledgement of their understanding and willingness to comply with these policies and procedures.	No exceptions noted.
1.3	Orders processed through the help desk are verified via phone for new customers, as evidenced by a note to a ticket in the ticketing system.	Inspected a sample of new client setup orders to determine that orders processed through the help desk were verified via phone for new customers, as evidenced by a note to a ticket in the ticketing system.	No exceptions noted.
1.4	Requests for new customer setup and changes to existing customer setup are monitored on a real-time basis.	Inspected a sample of new customer setups to determine that requests for new customer setups were monitored on a real-time basis.	No exceptions noted.

CONTROL AREA 1 **New Customer Setup and Maintenance**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.5	A customer support ticket is completed for each new customer setup and change to existing customer setup to help ensure accurate and timely completion of the account setup process.	Inspected a sample of existing customer setups to determine that requests for changes to existing customer setup were monitored on a real-time basis.	No exceptions noted.
		Inspected a sample of customer support tickets to determine that a customer support ticket is completed for each new customer setup to help ensure accurate and timely completion of the account setup process.	No exceptions noted.
		Inspected a sample of customer support tickets to determine that a customer support ticket is completed for each change to an existing customer setup to help ensure accurate and timely completion of the account setup process.	No exceptions noted.

CONTROL AREA 2 **Customer Support - Business Problems**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that production and business problems are identified, recorded, analyzed, and resolved completely and in a timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	The customer ticketing system allows customers as well as system administrators to initiate tickets relating to incidents.	Observed the access to initiate tickets within the customer ticketing system to determine that the customer ticketing system allowed customers as well as system administrators to initiate tickets relating to incidents.	No exceptions noted.
2.2	The customer is notified when a ticket is closed.	Inspected a sample of customer support tickets to determine that a customer was notified when a ticket was closed.	No exceptions noted.
2.3	Work on accounts is authorized by contacts listed within the customer management system.	Inquired of the Chief Financial Officer regarding authorized client contacts to determine that work on accounts was authorized by contacts listed within the customer management system.	No exceptions noted.
		Inspected a sample of customer tickets to determined that work on accounts was authorized by contacts listed within the customer management system.	No exceptions noted.
2.4	Problem tickets are worked through to resolution. Urgent tickets are left open for escalation procedures to ensure the necessary steps are taken and the appropriate personnel are contacted to obtain further instructions, as necessary.	Inspected a sample of problem tickets to determine that problem tickets were worked through to resolution and urgent tickets were left open for escalation procedures to ensure the necessary steps were taken and the appropriate personnel were contacted to obtain further instructions, as necessary.	No exceptions noted.
2.5	Authorized customer contacts are documented within the customer portal database, for use by datacenter personnel. Changes to the authorized customer contacts are logged.	Observed the customer portal database to determine that authorized customer contacts were documented within the customer portal database, for use by datacenter personnel.	No exceptions noted.

CONTROL AREA 2 **Customer Support - Business Problems**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that production and business problems are identified, recorded, analyzed, and resolved completely and in a timely manner.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the customer portal database log for a sample of new customers to determine that changes to the authorized customer contacts were logged.	No exceptions noted.
2.6	The customer ticketing system allows customers to request changes to client devices. System administrators view tickets and handle them according to the Company's policies and procedures. Any changes are documented and logged within the ticketing system.	Observed the access to initiate tickets within the customer ticketing system to determine that the customer ticketing system allowed customers to request changes to client devices, system administrators viewed tickets and handled them according to the entities policies and procedures and any changes were documented and logged within the ticketing system.	No exceptions noted.
		Inspected the customer ticketing queue to determine that the customer ticketing system allowed customers to request changes to client devices, system administrators viewed tickets and handled them according to the Company's policies and procedures, and any changes were documented and logged within the ticketing system.	No exceptions noted.
2.7	All open tickets are the responsibility of all system administrators while on duty.	Inspected a sample of problem tickets to determine that all open tickets were the responsibility of all system administrators while on duty.	No exceptions noted.
2.8	Ticket monitoring helps ensure that system administrators are aware of any open tickets and staff emails are used to communicate detailed information concerning the status of all open tickets at the end of each shift.	Inspected a sample of daily shift reports to determine that ticket monitoring helped ensure that system administrators were aware of any open tickets and staff emails were used to communicate detailed information concerning the status of all open tickets at the end of each shift.	No exceptions noted.

CONTROL AREA 3 **Customer Support - System Availability**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system availability is monitored, and issues are identified and resolved on a timely basis.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	The data center maintains redundant links to the Internet to help ensure service continually.	Inspected the live traffic load map to determine that the data center maintained redundant links to the Internet to help ensure service continually.	No exceptions noted.
		Inspected the carrier threshold monitoring configuration to determine that the data center maintained redundant links to the Internet to help ensure service continually.	No exceptions noted.
3.2	Wide area network links are monitored at the physical and logical levels including but not limited to link status, latency, packet-loss, capacity, and BGP status.	Inspected the carrier threshold monitoring configuration / status report to determine that wide area network links were monitored at the physical and logical levels including but not limited to link status, latency, packet-loss, capacity, and BGP status.	No exceptions noted.
3.3	The status of availability to the system is monitored via network ping testing. Availability monitoring takes place, at a minimum, every five minutes.	Inspected network ping test configuration and monitoring logs to determine that the status of availability to the system was monitored via network ping testing and availability monitoring took place, at a minimum, every five minutes.	No exceptions noted.
3.4	Monitoring logs are retained for at least a year.	Inspected the monitoring logs to determine that monitoring logs were retained for at least a year.	No exceptions noted.
3.5	Redundant monitoring of wide area network links is performed from both local and remote locations utilizing different network carriers.	Inspected evidence of the live traffic load map to determine that redundant monitoring of wide area network links was performed from both local and remote locations utilizing different network carriers.	No exceptions noted.
3.6	Core network services are run in high availability mode and/or an onsite spare device is available in the event of equipment failure.	Observed inventory of core network devices to determine that core network services were run in high availability mode and/or an onsite spare device was available in the event of equipment failure.	No exceptions noted.

CONTROL AREA 3 **Customer Support - System Availability**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that system availability is monitored, and issues are identified and resolved on a timely basis.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.7	Routing and switching products are used to provide full redundancy.	Inspected the live traffic load map to determine that routing and switching products were used to provide full redundancy.	No exceptions noted.
3.8	The IRP console is utilized to optimize overall network routing and performance. It monitors up to 150,000 prefixes exchanging traffic with Steadfast Networks' network for packet-loss and latency and makes adjustments to the BGP routing tables automatically as needed.	Inspected the IRP console to determine that the IRP console was utilized to optimize overall network routing and performance and monitored up to 150,000 prefixes exchanging traffic with Steadfast Networks' network for packet-loss and latency and made adjustments to the BGP routing tables automatically as needed.	No exceptions noted.
3.9	10 Gigabit Ethernet is used at the core of the network to reduce the risks of internal congestion due to distributed denial-of-service (DDoS) attacks and to maintain optimal flexibility.	Inspected a sample vendor order confirmation and vendor invoice for Ethernet service to determine that a 10 Gigabit Ethernet was used at the core of the network to reduce the risks of internal congestion due to distributed denial-of-service (DDoS) attacks and to maintain optimal flexibility.	No exceptions noted.
3.10	All core network devices are dual corded to redundant power circuits from separate Uninterruptible Power Supply (UPS) feeds.	Inspected a dual corded network router to determine that all core network devices were dual corded to redundant power circuits from separate UPS feeds.	No exceptions noted.
3.11	A change management process is followed for any maintenance performed on the routers and such maintenance is performed during a scheduled or emergency maintenance window.	Inspected the most recent router maintenance documentation to determine that a change management process was followed for any maintenance performed on the routers and such maintenance was performed during a scheduled or emergency maintenance window.	No exceptions noted.

CONTROL AREA 4 **Information Security**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	SSH access is executed via public key authentication, enabling the avoidance of using shared passwords and allows Steadfast Networks to restrict access to only users with private keys.	Inspected SSH access via public key authentication configuration to determine that SSH access was executed via public key authentication, enabling the avoidance of using shared passwords and allowed Steadfast Networks to restrict access to only users with private keys.	No exceptions noted.
4.2	Password access to server command lines is disabled for root as applicable. Inquired of management regarding SSH root access management to determine that password access to server command lines was disabled for root as applicable.	Inquired of the Chief Technology Officer regarding SSH root access management to determine that password access to server command lines was disabled for root as applicable.	No exceptions noted.
		Inspected SSH access via public key authentication configuration to determine that password access to server command lines was disabled for root as applicable.	No exceptions noted.
4.3	Key access is limited only to systems that a given staff member needs to do his/her job. Compromised keys are revoked immediately.	Inspected evidence of key access to a sample server to determine that key access was limited only to systems that a given staff member needed to do his/her job and compromised keys were revoked immediately.	No exceptions noted.
4.4	New user access to systems and data requires the completion of an access authorization form and approval by management personnel.	Inspected access authorization forms for a sample of new users to determine that new user access to systems and data required the completion of an access authorization form and approval by management personnel.	No exceptions noted.

CONTROL AREA 4 **Information Security**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.5	Internal servers are firewalled to limited IP ranges, except where specific services need to be exposed to the public. Access control lists deny access to administrative areas.	Inquired of the Chief Technology Officer regarding internal server access management to determine that internal servers were firewalled to limited IP ranges, except where specific services need to be exposed to the public and access control lists denied access to administrative areas.	No exceptions noted.
		Inspected firewall rulesets to determine that internal servers were firewalled to limited IP ranges, except where specific services need to be exposed to the public.	No exceptions noted.
		Inspected firewall administrator access list to determine that access control lists denied access to administrative areas.	No exceptions noted.
4.6	Internal systems use Secure Sockets Layer (SSL) protocol for any pages which submit or display sensitive data or accept login data. A minimum of 256-bit encryption is used.	Inspected the SSL server certificate for a sample of servers to determine that internal systems used Secure Sockets Layer (SSL) protocol, a cryptographic protocol, for any pages which submit or display sensitive data or accept login data and a minimum of 256-bit encryption was used.	No exceptions noted.
4.7	Staff members are given Virtual Private Network (VPN) key and certificate pairs for encrypted access from external sites. VPN certificates are revoked if compromised or if the staff member is terminated.	For a sample of terminated employees, inspected the access terminations forms and the VPN access listing to determine that VPN access was revoked if compromised or if the staff member was terminated.	No exceptions noted.
4.8	Certain shared passwords, only used when vendors do not have SSH key available, are rotated when compromised or staff changes occur.	Inspected evidence of a changed password to determine that shared passwords were rotated when a vendor was compromised, or staff changes occurred.	No exceptions noted.

CONTROL AREA 4 **Information Security**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.9	Administrative level accounts are granted only when staff members need to perform administrative tasks.	Inquired of the Chief Technology Officer regarding administrative account access to determine that administrative level accounts were granted only when staff members needed to perform administrative tasks.	No exceptions noted.
		Inspected a list of administrative level accounts to determine that administrative level accounts were granted only when staff members needed to perform administrative tasks.	No exceptions noted.
4.10	Staff login accounts are removed when a staff member's employment is terminated.	For a sample of terminated employees, inspected access termination forms, and the Ubersmith and OnApp access listings to determine that staff login accounts were removed when a staff member's employment was terminated.	No exceptions noted.
4.11	Customer information, such as password, server IDs and IP addresses are not written or printed.	Observed the support operations center where support personnel work to determine that customer information such as password, server IDs, and IP addresses were not written down or printed.	No exceptions noted.
4.12	Vulnerability scans are performed at least semi-annually.	Inspected a sample of semi-annual external vulnerability scans to determine that vulnerability scans were performed at least semi-annually.	No exceptions noted.
4.13	Daily log reviews of internal systems are sent to the email account of the CTO and are reviewed as necessary. Failed login attempts are logged and reviewed as necessary.	Inquired of the Chief Technology Officer regarding log review procedures to determine that daily log reviews of internal systems were sent to the email account of the CTO and were reviewed as necessary. Failed login attempts were logged and reviewed as necessary.	No exceptions noted.

CONTROL AREA 4 **Information Security**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the daily log reports to determine that daily log reviews of internal systems were sent to the email account of the CTO and were reviewed as necessary. Failed login attempts were logged and reviewed as necessary. Inspected the Ubersmith failed login log to internal system for a sample of days to determine that a daily log was generated. Failed login attempts were logged and reviewed as necessary.	No exceptions noted. No exceptions noted.

CONTROL AREA 5 **Change Management**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new implementation of and changes to infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Documented change management policies and procedures are in place to guide changes to customer services.	Inspected change management policies and procedures to determine that documented change management policies and procedures were in place to guide changes to customer services.	No exceptions noted.
5.2	Authorized customer contacts are documented within the customer portal database, for use by datacenter personnel. Changes to the authorized customer contacts are logged.	Observed the customer portal database to determine that authorized customer contacts were documented within the customer portal database, for use by datacenter personnel.	No exceptions noted.
		Inspected the customer portal database log for a sample of new customers to determine changes to the authorized customer contacts were logged.	No exceptions noted.
5.3	The customer portal allows customers to view devices, reboot/power down devices, add users, change status of users, and view bandwidth usage. Any changes are documented and logged in the customer portal.	Observed customer access to the portal to determine that the customer portal allowed customers to view devices, reboot/power down devices, add users, change status of users, and view bandwidth usage. Any changes were documented and logged in the customer portal.	No exceptions noted.
		Inspected the customer portal database log for a sample of new customers to determine that the customer portal allowed customers to view devices, reboot/power down devices, add users, change status of users, and view bandwidth usage. Any changes were documented and logged in the customer portal.	No exceptions noted.

CONTROL AREA 5 **Change Management**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new implementation of and changes to infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.4	The customer ticketing system allows customers to request changes to client devices. System administrators view tickets and handle them according to the Company's policies and procedures. Any changes are documented and logged within the ticketing system.	Observed access to initiate tickets within the customer ticketing system to determine that the customer ticketing system allowed customers to request changes to client devices, system administrators viewed tickets and handled them according to the Company's policies and procedures and any changes were documented and logged within the ticketing system.	No exceptions noted.
		Inspected a sample of customer tickets to determine that the customer ticketing system allowed customers to request changes to client devices. System administrators viewed tickets and handled them according to the entity's policies and procedures. Any changes were documented and logged within the ticketing system.	No exceptions noted.
5.5	Changes to client devices are made only when requests come from or are approved by authorized contacts.	Inspected a sample of customer request tickets to determine that changes to client devices were made only when requests came from or were approved by authorized contacts.	No exceptions noted.
5.6	Open tickets are the responsibility of all system administrators while on duty. Ticket monitoring helps ensure that system administrators are aware of any open tickets. Staff emails are used to communicate detailed information concerning the status of all open tickets at the end of each shift.	Inspected the customer ticketing queue to determine that open tickets were the responsibility of all system administrators while on duty, ticket monitoring helped ensure that system administrators were aware of any open tickets, and staff emails were used to communicate detailed information concerning the status of all open tickets at the end of each shift.	No exceptions noted.

CONTROL AREA 5 **Change Management**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new implementation of and changes to infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected a sample of daily shift reports to determine that open tickets were the responsibility of all system administrators while on duty, ticket monitoring helped ensure that system administrators were aware of any open tickets, and staff emails were used to communicate detailed information concerning the status of all open tickets at the end of each shift.	No exceptions noted.
5.7	Upon customer submission of a work order, tickets are assigned to an internal operator for handling.	Inspected a sample of work order tickets to determine that upon customer submission of a work order, tickets were assigned to an internal operator for handling.	No exceptions noted.
5.8	Customers are communicated to when a submitted work order ticket is completed.	Inspected a sample of work order tickets to determine that customers were communicated to when a submitted work order ticket was completed.	No exceptions noted.
5.9	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.
5.10	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Chief Technology Officer regarding access to implement changes in the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		Inspected a list of accounts with access to implement changes in the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.

CONTROL AREA 5 **Change Management**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that new implementation of and changes to infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.11	System change requests are documented and tracked in a ticketing system.	Inspected the change tickets for a sample of system changes to determine that system change requests are documented and tracked in a ticketing system.	No exceptions noted.

CONTROL AREA 6 **Computer Operations**

Control Objective Specified by the Service Organization: Controls provide reasonable assurance that timely system backups of critical files to an offsite location are performed.

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Backups to internal systems are performed at least daily to an off-site location. Backups are retained for at least two weeks.	Inspected the backup policy for internal systems to determine that backups to internal systems were performed at least daily to an off-site location and backups were retained for at least two weeks.	No exceptions noted.
		Inspected the backup schedule and configurations to determine that backups to internal systems were performed at least daily to an off-site location.	No exceptions noted.
		Inspected the detailed retention schedule to determine that backups to internal systems were retained for at least two weeks.	No exceptions noted.
6.2	Router and switch configuration backups are automatically performed hourly.	Inspected the log of a router configuration backup to determine that router and switch configuration backups were automatically performed hourly.	No exceptions noted.
6.3	Backup restoration tests from backup media are performed on at least annually.	Inspected backup restoration policies and procedures to determine that restoration tests were performed at least annually.	No exceptions noted.
		Inspected the most recent backup restoration to determine that backup restoration tests from backup media were performed at least annually.	No exceptions noted.
6.4	Backup e-mail notifications are provided by the backup software on a daily basis.	Inspected a sample of daily backup e-mail notifications to determine backup email notifications were provided by the backup software on a daily basis.	No exceptions noted.