INTERNAP®

March 25, 2014

Dear Valued Internap Customer,

In 2013, Internap initiated a project to upgrade our Access Control System for our company-controlled data centers. This project scope involved updating both hardware and software to achieve a state-of-the-art automated security system with much greater functionality and reporting capabilities. Although we engaged a third party technical service provider to lead our system upgrade, the appropriate quality control measures were not put in place to ensure the integrity of the data migration. During our annual SOC 2 audit process, we identified that five data centers incurred a time gap between the information migrated from the old system to the new system. Upon identification of this issue, we immediately reconciled and corrected the data, as well as remediated the gap for future conversions by creating a new control procedure. Our new control states, "Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy the migrated data." This reconciliation has taken place for all data center migrations occurring after October 1, 2013.

Although a time gap occurred, it is important to note that the conversion did not result in any inappropriate access to our data centers or cause any security incidents. All of our other security controls operated as designed, providing our customers with a safe, secure environment throughout the period.

As stated above, we have remediated this issue to ensure there is no data integrity gap. Additionally, to show our customers our commitment to operating excellence we engaged our external audit firm to perform a short-period audit at each site that was converted to the new Access Control System where the gap was identified. We are pleased to report that each of these sites received an unqualified audit opinion.

Please review the enclosed SOC 2 audit reports and reach out to us with any follow up questions.

Regards,

Steve Orchard
SVP & GM, Data Center and Network Services

Enclosures

SOC 2 Report – Seattle, WA

(SEF)

October 1, 2013 – January 31, 2014

Independent Service Auditor's Report

INTERNAP NETWORK SERVICES CORPORATION

Company-Controlled Data Center Services

Type 2 Report on Controls at a Service Organization
Relevant to Availability (SOC 2)

UHY LLP
Certified Public Accountants

INTERNAP®

INTERNAP NETWORK SERVICES CORPORATION

Report on Controls at a Service Organization Relevant to Availability Principle

TABLE OF CONTENTS

UHY LLP
Certified Public Accountants

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of
Internap Network Services Corporation

Scope

We have examined Internap Network Services Corporation's description of its system for providing Company-Controlled Data Center Services for the SEF facility in Seattle, Washington throughout the period October 1, 2013 to January 31, 2014 and the suitability of the design and operating effectiveness of controls to meet the criteria for the Availability Principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, throughout the period October 1, 2013 to January 31, 2014. 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 Internap Network Services Corporation's ("Internap" or "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.

Service organization's responsibilities

In Section II of this report, Internap 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. Internap is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of both the description and the assertion; providing the services covered by the description; specifying the controls that meet the applicable trust services criteria and stating them in the description; and designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Internap'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 October 1, 2013 to January 31, 2014.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of 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.

Inherent limitations

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.

UHY LLP
Certified Public Accountants

I. INDEPENDENT SERVICE AUDITOR'S REPORT

Opinion

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

a. The description fairly presents the SEF system that was designed and implemented throughout the period October 1, 2013 to January 31, 2014.

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 October 1, 2013 to January 31, 2014 and user entities applied the complementary user entity controls contemplated in the design of Internap's controls throughout the period October 1, 2013 to January 31, 2014.

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period October 1, 2013 to January 31, 2014.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of our tests are presented in Section IV of this report titled "Information Provided by the Independent Service Auditors."

Restricted use

This report, including the description of tests of controls and results thereof presented in Section IV of this report, is intended solely for the information and use of Internap; user entities of Internap's SEF system during some or all of the period October 1, 2013 to January 31, 2014; 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 services provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and 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.

UHY LLP

Atlanta, Georgia
March 24, 2014

II. MANAGEMENT'S ASSERTION

Internap Network Services Corporation's Assertion:

We have prepared the description of Internap's system for providing SEF Company-Controlled Data Center Services for the period October 1, 2013 to January 31, 2014. The description is intended to provide users with information about the system for providing SEF Company-Controlled Data Center Services, particularly system controls intended to meet the criteria for the Availability principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*). We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the system for providing SEF Company-Controlled Data Center Systems throughout the period October 1, 2013 to January 31, 2014, based on the following description criteria:

  i. The description contains the following information:

    (1) The types of services provided

    (2) The components of the system used to provide the services, which are the following:
    - *Infrastructure*. The physical and hardware components of the system (facilities, equipment, and networks).
    - *Software*. The programs and operating software of the services (systems, applications, and utilities).
    - *People*. The personnel involved in the operation and use of the system.
    - *Procedures*. The automated and manual procedures involved in the operation of the system.
    - *Data*. The information used and supported by the system (transaction streams, files, databases, and tables).

    (3) The boundaries or aspects of the system covered by the description

    (4) How the system captures and addresses significant events and conditions

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

    (6) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user entity controls contemplated in the design of the service organization's system

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

    (8) 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

    (9) 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 Internap's SEF 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 period October 1, 2013 to January 31, 2014 to meet the applicable trust services criteria.

c) the controls stated in the description operated effectively throughout the period October 1, 2013 to January 31, 2014 to meet the applicable trust services criteria.

III. DESCRIPTION OF THE INTERNAP NETWORK SERVICES CORPORATION SYSTEM – SEATTLE, WA (SEF) DATA CENTER SERVICES

Company Background and Service Offerings

Internap is the high-performance Internet infrastructure provider that powers the applications shaping the way we live, work and play. Our hybrid infrastructure delivers performance without compromise – blending virtual and bare-metal cloud, hosting and colocation services across a global network of data centers, optimized from the application to the end user and backed by rock-solid customer support and a 100% uptime guarantee.

Internap operates in two business segments: IP services; and data center services. The scope of this report excludes IP Services and focuses on data center services, which primarily include physical space for hosting customers' network and other equipment plus associated services such as redundant power, environmental controls and security.

Internap uses a combination of facilities that are operated by Internap and by third parties, referred to as company-controlled facilities and partner sites, respectively. We charge monthly fees for data center services based on the amount of square footage and power that a customer uses. This report is related to the SEF company-controlled data center.

The Aspects of the System and a Description of its Boundaries

Internap is primarily responsible for the following types of activities related to our data center services at the Seattle, WA (SEF) company-controlled facility:

- Providing a safe, secure facility for our customers. Related security requirements are supported by badge access systems, video surveillance cameras, an on-site 24 / 7 / 365 manned security desk, and controls designed to ensure that only authorized individuals have access to the facility.
- Ensuring that networks and systems are available for use by customers, as defined by service level agreements (SLAs) agreed to in advance with the customer. Availability requirements are supported by an environmentally stable facility with uninterruptable power for our customers. Environmental controls and redundancy features must be periodically serviced and maintained to ensure effective operation.
- Resolving customer complaints, issues, and incidents on an as needed basis, or providing administrative services that customers require to maintain the availability and related security of their systems.
- Consistently applying an infrastructure change management process designed to ensure that only authorized, adequately planned, and supervised changes to the facility are performed.

Internap provides the following customer support services, which enhance the availability and related security of the system by communicating related issues and requests with the customer. These services are primarily carried out by Network Operations Center (NOC) personnel.

- Responding to requests for support services.
- Responding to requests for changes (additions, modifications, and removals) to the customer's list of designated contacts. Requests for changes to customer contacts that have physical access are handled using this process.
- Responding to, and escalating, customer complaints and issues regarding the availability and/or related security of their services.

The Aspects of the System and a Description of its Boundaries *(Continued)*

Internap is not responsible for providing the following services for its colocation customers, unless these services are agreed to in advance under Internap's other service offerings (IP services, cloud services, hosting services, or hybridized services), which are not included within the scope of this report. Customers are responsible for performing these functions.

- Applying logical access security controls, including user authentication, password complexity requirements, password history requirements, password change procedures, account lockout procedures, and related procedures.
- Protecting and maintaining the network security of system resources (for example, secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services).
- Maintaining system components and configurations, including the application of change controls and procedures as necessary.
- Data encryption controls and the secure transfer of data through networks, including public, semi-private, and virtual private networks.
- Performing data backup procedures and data classification procedures as necessary.
- Protecting systems against infection by computer viruses, malicious codes, and unauthorized software.

Customers may choose to have Internap perform certain of these functions through Internap's other service offerings, which are not included within the scope of this report.

Risk Assessment

Internap utilizes various protocols to manage risks that could impact the Company's ability to deliver service to customers. Management also assesses risks that inherently arise from the expansion of the business, whether organically or inorganically. This may include managing risks that are rooted in changes in personnel, technology, or the Company's operating environment. Additionally, management engages a third party to periodically assess risks to the achievement of availability objectives. Management revisits this assessment annually to ensure risks are appropriately mitigated. Lastly, management performs an annual companywide risk assessment, which includes company-controlled data centers.

Information and Communication Systems

Internap's management team is responsible for the detailed design and effective operation of the Company's internal controls. As part of this process, management communicates responsibilities and expectations to company personnel through both formal and informal means. Internal controls are evaluated by Internal Audit throughout the year as part of its internal audit reviews. Testing results and exceptions identified during the audits are reported to management on a consistent basis. Management ensures that internal control deficiencies are addressed and communicates expected timelines for doing so.

Monitoring

Internap's management team, including support from its Internal Audit department, continuously monitors the effectiveness of the Company's system of internal control through the performance of periodic and annual audits of internal controls. Any deficiencies in the Company's system of internal controls are reported to management, assessed, and addressed. Management's consistent oversight of internal controls helps the Company identify deficiencies in the system, ensuring the adequacy of the process. Additionally, management has implemented availability monitoring controls in the form of external inspection, metrics reviews, and incident monitoring.

Control Environment and Policy and Procedural Components

Internap data center operational policies and procedures are documented in various ways and are readily available to employees and customers. The responsibility and accountability for developing and maintaining these polices, and changes and updates to these policies are assigned to the appropriate data center employees. Additionally, the information in these policies is reviewed on an annual basis by appropriate data center employees. The information in these policies relates to the specific Availability criteria from the Trust Principles and Criteria, including, but not limited to: identifying and documenting the system availability and related security requirements of authorized users; assessing risks on a periodic basis; preventing unauthorized access; adding new users, modifying the access levels of existing users, and removing users who no longer need access; assigning responsibility and accountability for system availability and related security; assigning responsibility and accountability for system changes and maintenance; testing, evaluating, and authorizing system components before implementation; addressing how complaints and request relating to system availability and related security issues are resolved; identifying and mitigating system availability and related security breaches and other incidents; providing training and other resources to support the system availability and related security policies; providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies; recovering and continuing service in accordance with documented customer commitments or other agreements; and monitoring system capacity to achieve customer commitments or other agreements regarding availability.

Each Internap data center has a specific Data Center Operations Manual kept in a binder and physically available to employees in case of an emergency. The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis to ensure the information is up-to-date and accurate.

The Network Operations Center (NOC) utilizes its own intranet webpage dedicated to its policies and procedures. Content is updated in real time on the intranet webpage to ensure NOC employees are always aware of the newest policy or procedures. On an annual basis, NOC management performs a review of information on the NOC intranet webpage to ensure the information is up-to-date and accurate. The NOC utilizes a ticketing system to track all incidents and customer requests. On a monthly basis, ticket resolution metrics are prepared and presented to Operations Management.

Each customer in Internap data centers is given a Service Level Agreement (SLA) and Customer Colocation Handbook with all necessary customer facing information and procedures to follow for many common questions/requests, such as system availability issues and what to do when a possible security breach is identified, along with many other incident responses. The information in the Customer Colocation Handbook is reviewed on an annual basis by data center management to ensure the information is up-to-date and accurate. Additionally, Internap customers connect to Internap via the Internap website and online customer portal. Our website hosts a detailed description of our data center services and the portal houses customer specific information and enables customers to contact Internap directly through the system. This customer portal, along with ad hoc communication methods are utilized to ensure transparent communication with customers. The description of Internap data center operations can be broken down into the specific components of Infrastructure, Software, People, and Procedures.

Infrastructure, Environmental and System Monitoring Components

Internap’s data center operations consist of a strong physical infrastructure, including secure facilities featuring N+1 redundancy for both power and cooling, along with fire protection and system monitoring. The existing facility and environmental standards at the data centers are designed to ensure that uptime is maximized by providing redundancy to key facility and environmental systems to ensure that mechanical or electrical failures will not result in an outage.

Monitoring Environmental Conditions and Critical Work Authorizations

Data center environmental conditions are constantly monitored and reported via an automated Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor a BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. If any issues or incidents with these environmental systems arise, the console displays an alert and e-mails on-site data center personnel.

Internap has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our customers. Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are re-visited annually by Internap data center and operations management to assess the risk associated with the threats identified.

Smoke/Fire Detection

The smoke/fire detection system in the data centers comprises smoke detectors and either a particulate sampling system or a very early smoke detection apparatus (VESDA) system that detects smoke during the very early stages of combustion. The smoke detection system is the first line of defense against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room, and the BMS generates e-mail alerts to data center employees.

The smoke detection system is inspected and serviced at least annually to ensure effective operation.

Fire Suppression

The fire suppression system consists of a pre-action dry pipe system. The pre-action dry pipe system is designed to keep water out of the sprinkler system plumbing in the data center areas during normal operations. If smoke and/or excessive heat is detected, and a sprinkler fusible head melts as a result, water is pumped into the sprinkler systems for the affected zone(s) only. The BMS continuously monitors and reports the status of the fire suppression system.

The fire suppression systems are inspected and serviced at least annually to ensure effective operation.

Clean agent fire extinguishers are also provided throughout the data center for accessibility in the event of a fire within the data center (or elsewhere in the building).

Fire extinguishers are inspected and serviced at least annually to ensure effective operation.

Heating, Ventilation, and Air Conditioning (HVAC)

Multiple HVAC units control both temperature and humidity within the data center and are configured in a redundant formation to ensure operation continues if a unit fails. Temperature and humidity are maintained to current SLA standards. The HVAC units are monitored by the BMS within the facility control room and NOC.

HVAC units are inspected and serviced at least annually to ensure effective operation.

Utility Power and Backup Power Systems

The data center power is provided by feeds from the local utility to support daily operations. The power is channeled into a UPS system which conditions the power to be supplied to data center equipment. The UPS system allows for customers to opt for redundant N+1 power feeds to their equipment. In the event of a utility power outage, the UPS system seamlessly draws backup power from a battery farm which will supply power for 15 to 20 minutes until diesel generators power up. Internap maintains a sufficient on-site fuel reserve, which gives the generators capability to power the data center for at least 48 hours.

Utility Power and Backup Power Systems (Continued)

Each of Internap's Company controlled facilities maintain contracts with fuel companies for the delivery of fuel as needed.

The UPS systems and generators are inspected and serviced at least annually to ensure effective operation.

Personnel, Security and Software System Components

Internap's commitment to competence includes management's determination of the levels of competence and expertise required for each position in the data centers, ensuring highly technical and customer service focused data center employees. Internap provides 24/7 manned facilities with a host of security features designed to protect our customer's equipment and network connectivity. Internap controls ingress and egress using electronic keycard and/or biometric software. All cages and cabinets are securely locked and CCTV monitors and records activity within each facility.

Organizational Structure and Assignment of Authority and Responsibility

Internap has developed an organizational structure that adequately suits the nature and scope of its operations. The Company has developed organizational charts that internally convey employee reporting relationships, operational responsibilities, and the overall organizational hierarchy.

Human Resource Policies and Practices

Internap's human resource department has policies and established practices that govern the hiring, termination, evaluation, promotion, counseling, and compensation of current and prospective company employees. A documented set of human resource, operational, and financial policies and procedures, along with a complete list of internal controls are made available to applicable employees via the intranet. Detailed job descriptions and organizational charts convey the requirements for each position. Internap also facilitates employee development through annual evaluations, on-site training, a company-wide tuition reimbursement program, and the allocation of funds for other relevant training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with Internap. Newly hired data center employees receive training and are made aware of customer facing documents and other internal policies covering system security and availability. For terminated employees, Internap has a formal process for decommissioning access to company records and systems in a timely manner.

Security Staff

A contracted security company employs and provides Internap's data center security resources. Such outsourcing ensures consistency of training, performance, metrics, and supervision. Responsibilities of security include, but are not limited to the following.

- Monitoring of Physical Security Systems
- Loss Prevention
- Internal Investigations
- Security Policies and Procedures Compliance

Security Control Desk

All Internap data centers have a Security Control Desk to control access, monitor security alarms, monitor Closed-Circuit Television camera signals (CCTV), and support security-related operational activities 24/7/365. Security personnel are on-site 24 hours a day, 7 days a week, 365 days a year. The Security Control Desk possesses the following.

- Real-time monitoring of data center door alarms
- Real-time monitoring of data center CCTV cameras
- Centralized security service and emergency dispatch communications for Security Staff, as well as for local fire departments, police departments, and other emergency response resources
- Electrical power support for continuous operation of communications, lighting, CCTV, intrusion detection, and alarm monitoring equipment in the event of utility power loss

Surveillance and Monitoring

- Internap data centers employ a CCTV (Closed Circuit Television) to record and facilitate monitoring of the data center. Cameras are positioned to provide views of critical areas, including perimeter doors, main entrances and exits, shipping & receiving, and other areas of importance.
- Internap security desk personnel monitor the signals from the CCTV system. The desk is connected by secure cables to the cameras throughout the facility to permit both interior and exterior surveillance.
- Cameras are recorded on site via digital video recorders 24/7/365. These visual records are retained for at least 90 days to provide details of activity at Internap data centers.
- Internap provides dedicated 24/7/365 CPS (continuous power supply) and standby emergency power via generator to support security systems.

Access Control

Internap employs a computerized Access Control System (ACS) to control physical access to our data centers. The ACS utilizes proximity card readers with pin codes or biometrics to control access into perimeter doors, shipping & receiving areas, storerooms, and other critical areas. Customers and employees (including contractors and security guards) must follow formal access request and approval processes before physical access to our data centers is granted. Additional access control features are as follows.

- Access to the data center and other restricted areas is specifically limited to authorized individuals
- Internap access badges and/or biometrics are required to gain entry to critical areas.
- Customers, Vendors, Contractors and other Visitors must be sponsored by an Internap-approved host to gain access if not on the Customer-Approved List.
- All Customers, Vendors, Contractors, and Visitors on the Customer-Approved List must check in with the Security Desk upon arrival with a photo identification if they require the physical key to access cages. Those customers with badge cage access will have automatic access to their cages.
- Visitors and others not on the Customer-Approved List are escorted while in the data center and other critical areas.
- Guest access for approved Contractors is generally limited to particular areas where work is being performed. Long term contractors are granted more general access via personal badges.
- Employees with access to the data center are limited to those with a specific business need or job function.

Access Control (Continued)

Administrator access (add, modify and delete users) in the ACS is restricted to appropriate personnel based on job roles and responsibilities and reviewed during periodic access reviews. Data Center Management authorizes Administrator access to the keycard system based on the individuals' job responsibilities.

The ACS is also used to monitor, notify, and log security alarms. The system monitors the following.

- Perimeter/external doors
- Restricted area doors
- Data center doors
- Shipping/receiving doors

The system is programmed to log all card reader activity. It also generates alarms for forced doors, propped doors, and denied card read attempts.

Visitor/Sales Tour Access

All Internap data center tours must be coordinated with an Internap representative. Tours of the data center and other restricted areas require an escort from an authorized Internap employee.

Customer Access

Each customer is permitted to designate individuals with access to Internap data centers via the Network Operations Center (NOC). The customers make requests for access through the NOC via email, phone call, or the online Customer Portal. The NOC manages customers' respective Customer Access Lists (CAL) within the Ubersmith Facility Management application. Update access to the CAL is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to the CALs and will only allow individuals listed on a Company's CAL access to the data center. The customer is responsible for requesting additions, modification, or deletions to access; the NOC is responsible for management of the Customer Access List. Upon notification of a customer employee termination or revocation of customer agreement, physical access to the data center is revoked. Customers are responsible for retaining a terminated employees access badge and either destroying it or returning it to Internap security.

Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.

Cages are secured via one of two possible means: Physical key or electronic badge reader.

1. Physical key - Keys are maintained by Internap security personnel. After the security personnel determine appropriate authority per the CAL, they escort the customer to the cage and unlock it for them; or

2. Badge reader access - access is controlled via the ACS, similar to that of data center access.

Cabinets are secured via one of two possible means: Physical key or combination lock.

1. Physical key - Keys are maintained by Internap security personnel. After the security personnel determine appropriate authority per the Customer Access List, they escort the customer to the cabinet and unlock it for them; or

2. Combination lock - access is controlled via the use of a customer specific combination code.

Customers are responsible for ensuring their cage or cabinet is properly locked before leaving the facility.

Employee and Security Guard Access to Data Center

Access to the data center is restricted to only those Internap employees with a legitimate business need. Access, if temporarily required for other employees whose job functions do not necessitate access to the data center on a day-to-day basis, is granted on a case-by-case basis by the data center manager, and these employees must be escorted by data center personnel. Physical access to the data center is revoked upon termination of Internap employees, and security guards.

Contractor and Vendor Access to Data Center

Access to the data center is restricted to Contractors and Vendors with a legitimate business purpose. Access is granted with a daily temporary badge and logged with security unless the Contractor or Vendor will be on site for an extended period of time or multiple times over an extended period (i.e. multiple weeks). Data Center management will notify Security of an expected Contractor or Vendor, and if a Contractor or Vendor arrives unexpectedly, Security will contact Data Center management to gain approval for temporary access. Temporary access cards are returned to security prior to leaving our facilities. If a temporary badge is not returned at the end of the day, it is disabled in the system by Security. Physical access to the data center is revoked upon completion of the contractors' and/or vendors' duties.

General Visitor Rules

- All visitors must be escorted at all times by an authorized host or employee.
- Internap data center regulations must be strictly followed at all times. Any individual (including Internap employees) not adhering to these rules will be escorted from the data center by staff and/or security.
- Badges must be displayed at all times within the facility.

Customer and Employee Access Review

Internap data center personnel perform audits to validate the appropriateness of access permissions in the Access Control System (ACS). The following audits are performed quarterly by Data Center Operations management.

1. Customer Access permissions in the ACS are validated against the Ubersmith Facilities Access application.
2. Employee, Contractor and Security Guard access permission in the ACS are reviewed for appropriateness.
3. Employees with access to add, modify, and delete users in the ACS are reviewed for appropriateness.

Data Used and Supported by the System

Client Data

Internap does not manage client data or content. Clients are responsible for applying logical access security controls, network security controls, data encryption controls, and related procedures to protect their data, as well as performing data backup procedures and data classification procedures as necessary.

Data Managed by Internap

Listing of Customer Contacts – Internap maintains a listing of all customer contacts with approved access to the data center. The listing provides the privileges granted to each contact, including whether or not they have physical access, may request tech support, or add other contacts to the approved listing managed by Internap. Customers may request a report listing all individuals on this approved listing, as well as their privileges.

Data Managed by Internap (Continued)

Access Control System Records and Customer, Employee, Security Guard, and Contractor Key Badges – Internap maintains a listing of all individuals with physical access to the data center. This is managed using the key card system. Customers may request a report listing all individuals who have physical access to their cage or cabinet.

Access Logs – The badge access system maintains records of all physical access attempts to the data center (both successful and unsuccessful). Temporary visitor and contractor logs are maintained by the Security Desk.

Trust Services Criteria Determined to be Not Applicable

Our data center operations, as described above, address all of the applicable Trust Services criteria related to the Availability principle, with the exception of the following criteria that are not applicable to Internap's data center operations model:

3.4 – "Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies." Clients are responsible for performing data backup procedures as necessary and ensuring the integrity and security of those backups.

3.7 – "Procedures exist to protect against unauthorized access to system resources (specifically perimeter network security, remote access, and the like)." Clients are responsible for protecting and maintaining the security of system resources (e.g., secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services).

3.8 – "Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software." Clients are responsible for protecting their equipment against infection by computer viruses, malicious codes and unauthorized software.

3.9 – "Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks." Clients are responsible for applying data encryption controls to protect their data.

3.11 – "Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary." Clients are responsible for data classification procedures.

3.15 – "Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies." Clients are responsible for maintaining their own system components and configurations.

Additionally, components of other applicable Trust Services criteria related to the Availability principle associated with backups, access to system resources and configurations, network management and protection, virus protection, encryption, and data are not applicable to Internap's data center operations.

Each of the six criteria noted above is classified under our complementary user entity control considerations, as Internap is responsible for providing a safe, secure, environmentally stable facility with uninterruptable power and internet connectivity for our customers to house their network equipment.

Clients may choose to have Internap perform certain of these controls and functions through other service offerings, which are not included within the scope of this report.

Complementary User Entity Control Considerations

Internap systems were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain control objectives included in this report. Internap has considered the following user entity control considerations in developing the controls which are described in Section III of this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at Internap. User auditors should consider whether the following controls have been placed in operation at user organizations. This is not a comprehensive list of all controls that should be employed at user organizations.

- User organizations are responsible for understanding and complying with their contractual obligations. (all criteria)
- User organizations are responsible for ensuring the supervision, management, and control of the use of Internap's services by their personnel. (all criteria)
- User organizations are responsible for designating authorized individuals for access requests to Internap's data center. (criteria 3.6)
- User organizations are responsible for notifying Internap of terminated employees. (criteria 3.6)
- User organizations are responsible for retaining a terminated employee's access badge and either destroying it or returning it to Internap security. (criteria 3.6)
- User organizations are responsible for changing their cabinet combination lock password after individuals with knowledge of the current combination are terminated. (criteria 3.6)
- User organizations are responsible for periodically reviewing their Customer Access Lists. (criteria 3.6)
- User organizations are responsible for immediately notifying Internap of any actual or suspected information security breaches, including compromised user accounts. (criteria 3.6)
- User organizations are responsible for notifying Internap of changes made to technical or administrative contact information. (criteria 3.6)
- User organizations are responsible for ensuring their employees properly lock their cage or cabinet before leaving Internap facilities. (criteria 3.6)
- User organizations are responsible for applying logical access security controls, data encryption controls, and related procedures to their network connected equipment. (criteria 3.7, 3.9)
- User organizations are responsible for the logical protection of their data, including performing backup procedures and classification procedures as necessary. (criteria 3.4, 3.7, 3.11)
- User organizations are responsible for protecting their equipment against infection by computer viruses, malicious codes and unauthorized software. (criteria 3.8)
- User organizations are responsible for maintaining their own system components and configurations. (criteria 3.15)
- User organizations are responsible for protecting and maintaining the security of system resources (e.g., secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services). (criteria 3.15)

IV. INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITORS

A. Introduction

The accompanying description of the SEF Company-Controlled Data Center Services of Internap is intended to provide user organizations and their auditors with sufficient information to obtain an understanding of those aspects of the controls of Internap that may be relevant to their control structure. This document, when combined with an understanding of the controls in place by the client, is intended to assist in the assessment of the total control structure surrounding systems maintained by the Internap SEF Company-Controlled Data Center.

Our review of the controls as described below for the period October 1, 2013 to January 31, 2014, included such tests as we considered necessary in the circumstances to obtain evidence about their effectiveness in meeting the applicable trust services criteria. The procedures performed in our review include only testing or reviewing procedures with respect to the controls of the SEF Company-Controlled Data Center operations of Internap. Consequently, we make no representations as to the adequacy of the control environment relative to other functions at Internap.

The objective of a control structure is to provide reasonable, but not absolute, assurance as to the safeguarding of assets against loss from unauthorized use or disposition and the reliability of records. The concept of reasonable assurance recognizes that the cost of a control structure should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgments made by management. As part of our study of the control structure, we performed a variety of tests, each of which provided different levels of audit satisfaction. The results of these tests provided the basis for our understanding of the control structure, and whether the controls included in this document were in place and operating effectively to ensure that systems were Available in accordance with Internap's controls. The section below outlines the various tests applied.

Our examination of the operating effectiveness of the controls of Internap's SEF Company-Controlled Data Center Services was restricted to applicable trust services criteria as outlined below. The examination was performed in accordance with attestation standards established by the AICPA. It is each user entity's responsibility to evaluate this information in relation to the control structure surrounding the specific client under audit.

B. Control Environment

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) a review of Internap's organizational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals, personnel policies and the internal audit's policies; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of our testing of their controls to support our conclusions on the achievement of the applicable trust services criteria.

C. Control Objectives, Control Activities, Testing Performed and Testing Results

Our testing of the effectiveness of controls included the testing necessary, based upon our judgment, to evaluate whether adherence with those controls was sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria included below were achieved during the period October 1, 2013 to January 31, 2014. In selecting particular tests of the effectiveness of controls, we considered (a) the nature of items being tested, (b) the types and competence of available evidential matter, (c) the nature of the applicable trust services criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

C. Control Objectives, Control Activities, Testing Performed and Testing Results (Continued)

The tests performed on the effectiveness of controls detailed in the following section are described below:

TEST **DESCRIPTION**

Re-performance

Re-performed application of the control structure policy or procedure to ensure adequacy of its application. This includes, among other things, obtaining evidence of the arithmetical accuracy and correct processing of transactions by either re-computing Internap's computations or performing independent calculations.

Inspection

Inspected documents and reports that indicate performance of the control structure policy or procedures. This includes among other things:

- Testing of source documents to ensure transactions processed were consistent with transaction requests and that such transactions were in compliance with control structure policies.
- Reviewing of source documentation and authorization to verify propriety and timeliness of control activities performed.

Observation

Observed application of specific controls.

Inquiry

Made inquiries of the appropriate Internap staff. Inquiries seeking relevant information or representation from Internap personnel were performed to obtain:

- Knowledge and additional information regarding the policy and procedure.
- Corroborating evidence of the policy or procedure.

Internap Control Activities, Testing Steps Performed, and Results of Testing

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	Availability			
1.0	**Policies: Internap defines and documents its policies for the availability of its system.**			
1.1	The entity's policies for system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	A - A written Data Center Operations Manual, Network Operations Center Procedures, and Customer Colocation Handbook are in place documenting data center policies and procedures.	**Inspection** Inspected the manuals to verify that data center availability and security policies and procedures are documented and in place.	No exceptions noted.
		B - The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Data Center Operations Manual to verify that it was reviewed and approved by Data Center Operations management on an annual basis.	No exceptions noted.
		C - The Network Operations Center procedures are reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Network Operations Center procedures to verify that they were reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	No exceptions noted.
		D - The customer Colocation Handbook is reviewed and approved by the Colocation business unit management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Customer Colocation Handbook to verify that it was reviewed and approved by business unit management on an annual basis.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
1.2 The entity's system availability and related security policies include, but may not be limited to, the following matters: a. Identifying and documenting the system availability and related security requirements of authorized users. b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements. c. Assessing risks on a periodic basis. d. Preventing unauthorized access. e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access. f. Assigning responsibility and accountability for system availability and related security. g. Assigning responsibility and accountability for system changes and maintenance. h. Testing, evaluating, and authorizing system components before implementation. i. Addressing how complaints and	A - A written Data Center Operations Manual, Network Operations Center Procedures, and Customer Colocation Handbook are in place documenting data center policies and procedures.	**Inspection** Inspected the manuals to verify that data center availability and security policies and procedures are documented and in place.	No exceptions noted.
	B - The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Data Center Operations Manual to verify that it was reviewed and approved by Data Center Operations management on an annual basis.	No exceptions noted.
	C - The Network Operations Center procedures are reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Network Operations Center procedures to verify that they were reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	No exceptions noted.
	D - The customer Colocation Handbook is reviewed and approved by the Colocation business unit management on an annual basis.	**Inquiry** Inquired about the process for developing, approving and maintaining policies and procedures. **Inspection** Inspected the Customer Colocation Handbook to verify that it was reviewed and approved by business unit management on an annual basis.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
requests relating to system availability and related security issues are resolved. j. Identifying and mitigating system availability and related security breaches and other incidents. k. Providing for training and other resources to support its system availability and related security policies. l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies. m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements. n. Recovering and continuing service in accordance with documented customer commitments or other agreements. o. Monitoring system capacity to achieve customer commitments or other agreements regarding availability.	G - Customer on-boarding procedures include providing the new customer with a Colocation Handbook and SLA upon initiating service.	**Inquiry** Inquired of Internap personnel to determine whether new colocation customers are provided the Colocation Handbook and Service Level Agreement upon initiating service. **Inspection** Inspected the Colocation Handbook and Service Level Agreement to verify that they exist and include related availability and security obligations of users and Internap's availability and security commitments. Inspected the e-mail template for new customers to verify that procedures exist to instruct the business unit to provide the Colocation Handbook and Service Level Agreement to new customers.	No exceptions noted.
	L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected reports and results from the latest third-party data center risk assessment and annual data center strategy plan to verify that a third-party data center risk assessment had been reviewed and risks assessed within the past year.	No exceptions noted.
	M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment was performed within the past year. **Inspection** Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
1.3	Responsibility and accountability for developing and maintaining the entity’s system availability and related security policies, and changes and updates to those policies, are assigned.	E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry** Inquired of management to determine whether the organizational chart and job descriptions were updated within the past year. **Inspection** Inspected the Internap Organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.0	**Communications: Internap communicates its defined system availability policies to responsible parties and authorized users.**			
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	F - The Company has prepared a description of its colocation service offerings and posts it to the Company website for users to access.	**Observation** Observed Internap's external website to verify that a description of its colocation service offerings and system boundaries are posted.	No exceptions noted.
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	F - The Company has prepared a description of its colocation service offerings and posts it to the Company website for users to access.	**Observation** Observed Internap's external website to verify that a description of its colocation service offerings and system boundaries are posted.	No exceptions noted.
		G - Customer on-boarding procedures include providing the new customer with a Colocation Handbook and SLA upon initiating service.	**Inquiry** Inquired of Internap personnel to determine whether new colocation customers are provided the Colocation Handbook and Service Level Agreement upon initiating service. **Inspection** Inspected the Colocation Handbook and Service Level Agreement to verify that they exist and include related availability and security obligations of users and Internap's availability and security commitments. Inspected the e-mail template for new customers to verify that procedures exist to instruct the business unit to provide the Colocation Handbook and Service Level Agreement to new customers.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection** Inspected the Data Center Operations Manual to verify that it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	No exceptions noted.
	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
2.3 Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry** Inquired of management to determine whether the organizational chart and job descriptions were updated within the past year. **Inspection** Inspected the Internap Organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection** Inspected the Data Center Operations Manual to verify that it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	No exceptions noted.
	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
	J - The process for users (customers) to inform the entity of system availability issues, possible security breaches, and other incidents is documented in the "customer colocation handbook".	**Inspection** Inspected the Customer Colocation Handbook to verify that the process for customers to inform Internap of system availability issues, possible security breaches, and other incidents was documented.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
		K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes during the period, inspected Critical Environment Work Authorization (CEWA) forms to verify that the work had been properly reviewed and approved.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.0 **Procedures: Internap placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.**			
3.1 Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected reports and results from the latest third-party data center risk assessment and annual data center strategy plan to verify that a third-party data center risk assessment had been reviewed and risks assessed within the past year.	No exceptions noted.
	M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment was performed within the past year. **Inspection** Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year.	No exceptions noted.
3.2 Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	N - A smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire.	**Observation** Observed the smoke detection system in the data center to verify that a smoke detection system is installed in the data center.	No exceptions noted.
	O - The smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that the smoke detection system was inspected and serviced within the past year.	No exceptions noted.
	P - The data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers located throughout the data center.	**Observation** Observed fire suppression systems and fire extinguishers throughout the data center to verify that the data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected preventive maintenance and inspection reports to verify that the fire suppression system and fire extinguishers were inspected and serviced within the past year.	No exceptions noted.
	R - Multiple HVAC units control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	**Observation** Observed multiple HVAC units to verify that HVAC units are designed to control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	No exceptions noted.
	S - HVAC units are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that HVAC units were inspected and serviced within the past year.	No exceptions noted.
	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes during the period, inspected Critical Environment Work Authorization (CEWA) forms to verify that the work had been properly reviewed and approved.	No exceptions noted.
	T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to verify that redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that UPS systems were inspected and serviced within the past year.	No exceptions noted.
	V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to verify that multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
	W - Generators are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that generators were inspected and serviced within the past year.	No exceptions noted.
	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.3	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
		T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to verify that redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
		V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to verify that multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
3.5	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: a. Logical access security measures to restrict access to information resources not deemed to be public. b. Identification and authentication of users. c. Registration and authorization of new users. d. The process to make changes and updates to user profiles. e. Restriction of access to offline storage, backup data, systems,	Y - Data Center Management approves all provisioning of Administrator access (add, modify, delete users) to the keycard system.	**Inspection** Inspected a sample of approvals for administrative users added during the period to verify that access was approved by Data Center Management.	No exceptions noted.
		Z - On a quarterly basis, individuals with access to add, modify, and delete users in the key card system are reviewed for appropriateness.	**Inspection** Inspected a sample of quarterly audits to verify that Internap co-location security personnel perform quarterly audits to validate the appropriateness of individuals with access to add, modify, and delete users in the key card access system. Inspected the list of active users with access to add, modify, and delete users in the key card system to verify that users with inappropriate access to the system identified during quarterly audits were removed.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
and media. f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	AA - User access to edit the Facilities Access Customer Contact Lists in Ubersmith is reviewed for appropriateness based on job responsibilities on an annual basis.	**Inspection** Inspected the annual review of user access to edit the customer contact lists to verify that Internap personnel perform an annual review to validate the appropriateness of individuals with access to edit the customer contact lists in Ubersmith. Inspected the list of active users with access to edit the customer contact lists to verify that users with inappropriate access to the system identified during the annual review were removed.	No exceptions noted.
	OO - Internap colocation security personnel perform a quarterly audit to validate the appropriateness of all employee, contractor, and security guard physical access to the data centers.	**Inspection** Inspected a sample of quarterly audits of employees, contractors, and security guards with data center access to verify that the reviews to validate the appropriateness of employees, contractors, and security guards with access to data centers were reviewed. Inspected the keycard access listings to verify that users with inappropriate access to the system identified during quarterly audits were removed.	No exceptions noted.
	PP - Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy of the migrated data.	No migrations were performed for data center applications during the period under review. As a result, no testing was performed.	No exceptions noted.
3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	BB - Only authorized Internap employees, contractors, security guards, and customers are granted physical access to the data center.	**Inspection** Inspected a sample of approvals for employees, contractors, customers, and security guards who were granted physical access to the data center during the period to verify that only authorized Internap employees, contractors, and customers are granted physical access to the data center.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	CC - Physical access to the data center is revoked upon termination of Internap employees, contractors, and security guards.	**Inquiry** Inquired of a sample of third party service providers for Internap to determine whether physical access to data centers was revoked for contractors who were terminated during the period. **Inspection** Inspected the active keycard listing for a sample of terminated employees, contractors, and security guards to verify that physical access to the data center is revoked upon termination of Internap employees, contractors, and security guards.	No exceptions noted.
	DD - Physical access to the data center is revoked upon notification by customers to the NOC for customer employee terminations.	**Inspection** Inspected the keycard access listings for a sample of customer employees who required data center access revocation to verify that unauthorized customer employee access was removed.	No exceptions noted.
	EE - Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.	**Inquiry** Inquired of data center management to determine whether customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. **Observation** Observed locked cages and locked cabinets to verify that customer equipment is segregated via locked cages or locked cabinets such that customers can only access their own equipment.	No exceptions noted.
	FF - In order to gain physical access to Internap data centers, employees and customers must be validated via a combination of key card and biometric technology.	**Inquiry** Inquired of management to determine whether employees and customers must be validated by key card and biometric technology. **Observation** Observed successful and unsuccessful attempts to gain entry to the data center to verify that employees and customers must be validated by keycard and biometric technology.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	GG - A manned security post controls entry into Internap data centers. Customers must pass by the manned security post prior to gaining access to the data center.	**Inquiry** Inquired of data center management to determine whether a manned security post controls entry into Internap data centers. **Observation** Observed the manned security post that is placed in line of sight of where customers gain access to the data center to verify that a manned security post controls entry into Internap data centers.	No exceptions noted.
	JJ - Internap employs 24 hour video surveillance to monitor all entrances, exits, and other sensitive areas of its data centers. Surveillance video footage is retained for at least 90 days.	**Observation** Observed video surveillance cameras at entrances, exits, and sensitive areas, as well as security personnel monitoring video feeds to verify that sensitive locations are monitored by Internap personnel. Observed historical surveillance video footage to verify that recordings are retained for at least 90 days.	No exceptions noted.
	HH - Visitor access to Internap data centers is logged at the security desk.	**Inspection** Inspected security logs for a sample of days to verify that details of visitor access to Internap data centers is logged at the security desk.	No exceptions noted.
	OO - Internap colocation security personnel perform a quarterly audit to validate the appropriateness of all employee, contractor, and security guard physical access to the data centers.	**Inspection** Inspected a sample of quarterly audits of employees, contractors, and security guards with data center access to verify that the reviews to validate the appropriateness of employees, contractors, and security guards with access to data centers were reviewed. Inspected the keycard access listings to verify that users with inappropriate access to the system identified during quarterly audits were removed.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		II - Internap colocation security personnel perform a quarterly audit to validate the appropriateness of all customers' physical access to the data centers.	**Inspection** Inspected a sample of quarterly customer access audits to verify that Internap co-location security personnel perform a quarterly audit to validate the appropriateness of customers' physical access to the data centers.	No exceptions noted.
		PP - Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy of the migrated data.	No migrations were performed for data center applications during the period under review. As a result, no testing was performed.	No exceptions noted.
3.10	Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection** Inspected the Data Center Operations Manual to verify that it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.12	Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	O - The smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that the smoke detection system was inspected and serviced within the past year.	No exceptions noted.
		Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected preventive maintenance and inspection reports to verify that the fire suppression system and fire extinguishers were inspected and serviced within the past year.	No exceptions noted.
		S - HVAC units are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that HVAC units were inspected and serviced within the past year.	No exceptions noted.
		U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that UPS systems were inspected and serviced within the past year.	No exceptions noted.
		W - Generators are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that generators were inspected and serviced within the past year.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.
	L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected reports and results from the latest third-party data center risk assessment and annual data center strategy plan to verify that a third-party data center risk assessment had been reviewed and risks assessed within the past year.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment was performed within the past year. **Inspection** Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year.	No exceptions noted.
		KK - Tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether issue tracking ticket resolution metrics are reported on a monthly basis to operations management to monitor the timeliness of completion. **Inspection** For a sample of months, inspected the operations management reporting package to verify that ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.
3.13	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes during the period, inspected Critical Environment Work Authorization (CEWA) forms to verify that the work had been properly reviewed and approved.	No exceptions noted.
3.14	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.	LL - An employment pre-screening process is in place. It includes background, credit, and DMV checks (based on job requirements).	**Inspection** Inspected pre-screen results in the employee files for a sample of employees hired during the period to verify that an employment pre-screening process is in place and includes background, credit and DMV checks where applicable and based on job requirements.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	MM - An annual performance review process is in place. It gives managers and employees an opportunity to discuss performance, ethics, integrity, and training needs. The review process also includes setting goals and objectives for the following year.	**Inspection** Inspected documentation evidencing that the annual performance review process is in place and discusses ethics, integrity, training needs, along with setting goals for the upcoming year.	No exceptions noted.
	E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry** Inquired of management to determine whether the organizational chart and job descriptions were updated within the past year. **Inspection** Inspected the Internap Organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.
	NN - The Company allows operating units to budget training for each employee to continue their education either virtually or locally, including maintenance of certifications. The Company also has a formal tuition reimbursement program.	**Inspection** Inspected the Employee Handbook to verify that the Company allows operating units to budget training for each employee to continue education either virtually or locally, including maintenance of certifications, and whether the Company also has a formal tuition reimbursement program. Inspected Internap's operating budget for the current year to determine whether it included allowance for training and continuing education.	No exceptions noted.
3.16 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes during the period, inspected Critical Environment Work Authorization (CEWA) forms to verify that the work had been properly reviewed and approved.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.17 Procedures exist to provide that emergency changes are documented and authorized.	I - Each Internap Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to verify that it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes during the period, inspected Critical Environment Work Authorization (CEWA) forms to verify that the work had been properly reviewed and approved.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4	**Monitoring: Internap monitors the system and takes action to maintain compliance with its defined system availability policies.**			
4.1	The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.
		KK - Tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether issue tracking ticket resolution metrics are reported on a monthly basis to operations management to monitor the timeliness of completion. **Inspection** For a sample of months, inspected the operations management reporting package to verify that ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.
		N - A smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire.	**Observation** Observed the smoke detection system in the data center to verify that a smoke detection system is installed in the data center.	No exceptions noted.
		O - The smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that the smoke detection system was inspected and serviced within the past year.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected reports and results from the latest third-party data center risk assessment and annual data center strategy plan to verify that a third-party data center risk assessment had been reviewed and risks assessed within the past year.	No exceptions noted.
	M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment was performed within the past year. **Inspection** Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year.	No exceptions noted.
	P - The data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers located throughout the data center.	**Observation** Observed fire suppression systems and fire extinguishers throughout the data center to verify that the data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers.	No exceptions noted.
	Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected preventive maintenance and inspection reports to verify that the fire suppression system and fire extinguishers were inspected and serviced within the past year.	No exceptions noted.
	R - Multiple HVAC units control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	**Observation** Observed multiple HVAC units to verify that HVAC units are designed to control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	S - HVAC units are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that HVAC units were inspected and serviced within the past year.	No exceptions noted.
	T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to verify that redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
	U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that UPS systems were inspected and serviced within the past year.	No exceptions noted.
	V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to verify that multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
	W - Generators are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a preventative maintenance and inspection report to verify that generators were inspected and serviced within the past year.	No exceptions noted.
	KK - Tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether issue tracking ticket resolution metrics are reported on a monthly basis to operations management to monitor the timeliness of completion. **Inspection** For a sample of months, inspected the operations management reporting package to verify that ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.

	SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4.3	Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.	X - Data center environmental conditions are monitored and reported via the Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the Building Management System (BMS) and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to verify that power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Building Management System (BMS). Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the Building Management System (BMS) console to verify that the real-time status of power, HVAC, temperature, and fire detection/suppression conditions is being monitored by Internap personnel.	No exceptions noted.
		L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected reports and results from the latest third-party data center risk assessment and annual data center strategy plan to verify that a third-party data center risk assessment had been reviewed and risks assessed within the past year.	No exceptions noted.

SOC 2 Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment was performed within the past year. **Inspection** Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year.	No exceptions noted.

INTERNAP®

SOC 2 – Availability

Report on Internap Network Services Corporation's Description of its SEF Company-Controlled Data Center System and Suitability of Design and Operating Effectiveness of Controls Throughout the Period October 1, 2012 - September 30, 2013

The report on Internap Network Services Corporation's Description of its SEF Company-Controlled Data Center System and Suitability of Design and Operating Effectiveness of Controls is confidential. This report is intended solely for the use by the management of Internap Network Services Corporation, its user entities, prospective user entities, independent auditors and practitioners of its user entities, and regulators who have sufficient knowledge and understanding of the AICPA Availability Trust Principle, and is not intended and should not be used by anyone other than these specified parties.

Table of Contents

This report is intended solely for the use by the management of Internap Network Services Corporation and the specified parties, and is not intended and should not be used by anyone other than these parties.

Section I: Report of Independent Service Auditors

To: Management of Internap Network Services Corporation

Scope

We have examined the attached description titled "Description of Internap Network Services Corporation's SEF Company-Controlled Data Center System throughout the Period October 1, 2012 to September 30, 2013" (the "description") and the suitability of the design and operating effectiveness of controls to meet the criteria for the availability principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) ("applicable trust services criteria"), throughout the period October 1, 2012 to September 30, 2013. 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 Internap Network Services Corporation's ("Internap" or "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.

Service organization's responsibilities

Internap has provided the attached assertion titled "Management of Internap Network Services Corporation's Assertion Regarding its SEF Company-Controlled Data Center System Throughout the Period October 1, 2012 to September 30, 2013," which is based on the criteria identified in the management's assertion. Internap 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; (5) identifying any applicable trust service criteria related to the principle being reported on that have been omitted from the description and explaining the reason for the omission, and (6) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Internap'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 October 1, 2012 to September 30, 2013.

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.

Inherent limitations

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.

Basis for qualified opinion

Internap Network Services Corporation states in the description of its system it employs a computerized Access Control System (ACS) to control physical access to its data centers that house customer equipment, media and documentation. The ACS utilizes proximity card readers with pin codes or biometrics to control access into perimeter doors, shipping & receiving areas, storerooms, and other critical areas. In 2013, Internap upgraded the ACS to the most current version. This upgrade required a migration to new hardware and software to support the updated application. As noted in section IV, however, controls related to the reconciliation of ACS migrated user access data were not adequately performed and, therefore, control PP which was intended to reconcile migrated ACS user access data was not suitably designed to meet the following criteria:

3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

a. Logical access security measures to restrict access to information resources not deemed to be public.
b. Identification and authentication of users.
c. Registration and authorization of new users.
d. The process to make changes and updates to user profiles.
e. Restriction of access to offline storage, backup data, systems and media.
f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls

3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

Opinion

In our opinion, except for the matters referred to in the preceding paragraphs, based on the description criteria identified in Internap's assertion and the applicable trust services criteria, in all material respects,

a. the description fairly presents the SEF Company-Controlled Data Center System that was designed and implemented throughout the period October 1, 2012 to September 30, 2013.

b. the controls of Internap 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 October 1, 2012 to September 30, 2013, and user entities applied the complementary user-entity controls contemplated in the design of Internap's controls throughout the period October 1, 2012 to September 30, 2013.

c. the controls of Internap tested, which together with the complementary user-entity controls referred to in the scope section of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period October 1, 2012 to September 30, 2013.

Other information provided by the service organization

The information attached to the description titled "Other Information Provided by Internap Management" describes management's responses to testing exceptions identified. It is presented by the management of Internap to provide additional information and is not a part of the service organization's description of its SEF Company-Controlled Data Center System made available to user entities during the period from October 1, 2012, to September 30, 2013. Information included within the description titled "Other Information Provided by Management" has not been subjected to the procedures applied in the examination of the description of the SEF Company-Controlled Data Center System and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the description of the SEF Company-Controlled Data Center System.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Internap's Control Activities and PwC's Tests of Controls and Results."

Restricted use

This report and the description of tests of controls and results thereof are intended solely for the information and use of Internap; user entities of Internap's SEF Company-Controlled Data Center System during some or all of the period October 1, 2012 to September 30, 2012; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators (collectively referred to as "specified parties") 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. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

December 5, 2013
Atlanta, GA

Section II: Management of Internap Network Services Corporation's Assertion regarding its SEF Company-Controlled Data Center System Throughout the Period October 1, 2012 to September 30, 2013

We have prepared the attached description titled "Description of Internap Network Services Corporation's SEF Company-Controlled Data Center System Throughout the Period October 1, 2012 to September 30, 2013 (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 paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (*SOC2*^{SM}) (the "description criteria"). The description is intended to provide users with information about the SEF Company-Controlled Data Center System, particularly system controls intended to meet the criteria for the availability principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids) ("applicable trust services criteria"). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the SEF Company-Controlled Data Center System throughout the period October 1, 2012 to September 30, 2013, 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:
   (1) Infrastructure - The physical and hardware components of a system (facilities and equipment).
   (2) Software - The programs used to manage active customers and data center badge access.
   (3) People - The personnel involved in the operation and use of a system (operators, users, and managers).
   (4) Procedures - The automated and manual procedures involved in the operation of 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. 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

7. Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore

8. 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

9. 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. We state in the description of our system that we employ a computerized Access Control System (ACS) to control physical access to our data centers that house customer equipment, media and documentation. The ACS utilizes proximity card readers with pin codes or biometrics to control access into perimeter doors, shipping & receiving areas, storerooms, and other critical areas. In 2013, Internap upgraded the ACS to the most current version. This upgrade required a migration to new hardware and software to support the updated application. As noted in section IV, however, controls related to the reconciliation of ACS migrated user access data were not adequately performed and, therefore, control PP which was intended to reconcile migrated ACS user access data was not designed appropriately. This control deficiency resulted in not meeting the following Criteria:

3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

a. Logical access security measures to restrict access to information resources not deemed to be public.
b. Identification and authentication of users.
c. Registration and authorization of new users.
d. The process to make changes and updates to user profiles.
e. Restriction of access to offline storage, backup data, systems and media.
f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls

3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

c. except for the matters described above, the controls stated in the description were suitably designed and implemented throughout the period October 1, 2012 to September 30, 2013 to meet the applicable trust services criteria

d. the controls stated in the description operated effectively throughout the period October 1, 2012 to September 30, 2013 to meet the applicable trust services criteria.

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

Company Background

Internap (NASDAQ: INAP) provides cloud, hosting, colocation and hybridized services that are designed for superior performance and delivered from a geographically distributed platform of high-density, redundant data centers. Its patented, performance-optimized IP connectivity enables customers to focus on their core business, improve service levels and lower the cost of IT operations.

Internap operates in two business segments: IP services; and data center services. The scope of this report excludes IP Services and focuses on data center services, which primarily include physical space for hosting customers' network and other equipment plus associated services such as redundant power, environmental controls and security.

Internap uses a combination of facilities that are operated by Internap and by third parties, referred to as company-controlled facilities and partner sites, respectively. We offer a comprehensive solution, consisting of 12 company-controlled facilities for which SOC 2-Availability examinations are performed. We charge monthly fees for data center services based on the amount of square footage and power that a customer uses. This report is related to the SEF company-controlled data center.

Risk Assessment

Internap utilizes various protocols to manage risks that could impact the Company's ability to deliver service to customers. Management also assesses risks that inherently arise from the expansion of the business, whether organically or inorganically. This may include managing risks that are rooted in changes in personnel, technology, or the Company's operating environment. Additionally, management engages a third party to periodically assess risks to the achievement of availability objectives. Management revisits this assessment annually to ensure risks are appropriately mitigated. Lastly, management performs an annual companywide risk assessment, which includes company-controlled data centers.

Information and Communication Systems

Internap's management team is responsible for the detailed design and effective operation of the Company's internal controls. As part of this process, management communicates responsibilities and expectations to company personnel through both formal and informal means. Internal controls are evaluated by Internal Audit throughout the year as part of its internal audit reviews. Testing results and exceptions identified during the audits are reported to management on a consistent basis. Management ensures that internal control deficiencies are addressed and communicates expected timelines for doing so.

Monitoring

Internap's management team, including support from its Internal Audit department, continuously monitors the effectiveness of the Company's system of internal control through the performance of periodic and annual audits of internal controls. Any deficiencies in the Company's system of internal controls are reported to management, assessed, and addressed. Management's consistent oversight of internal controls helps the Company identify deficiencies in the system, ensuring the adequacy of the process. Additionally, management has implemented availability monitoring controls in the form of external inspection, metrics reviews, and incident monitoring.

Control Environment and Policy and Procedural Components

Internap data center operational policies and procedures are documented in various ways and are readily available to employees and customers. The responsibility and accountability for developing and maintaining these polices, and changes and updates to these policies are assigned to the appropriate data center employees. Additionally, the information in these policies is reviewed on an annual basis by the appropriate data center employees. The information in these policies relates to the specific Availability criteria from the Trust Principles and Criteria, including, but not limited to: identifying and documenting the system availability and related security requirements of authorized users; assessing risks on a periodic basis; preventing unauthorized access; adding new users, modifying the access levels of existing users, and removing users who no longer need access; assigning responsibility and accountability for system availability and related security; assigning responsibility and accountability for system changes and maintenance; testing, evaluating, and authorizing system components before implementation; addressing how complaints and requests relating to system availability and related security issues are resolved; identifying and mitigating system availability and related security breaches and other incidents; providing training and other resources to support the system availability and related security policies; providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies; recovering and continuing service in accordance with documented customer commitments or other agreements; and monitoring system capacity to achieve customer commitments or other agreements regarding availability.

Environmental controls regarding smoke detection, pre-action sprinkler suppression, HVAC, UPS, and generators are managed discretely at the SEF data center. However, other controls such as user access and data center monitoring are centrally managed by Internap across its company-controlled data centers.

Each Internap data center has a specific Data Center Operations Manual kept in a binder and physically available to employees in case of an emergency. The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis to ensure the information is up-to-date and accurate.

The Network Operations Center (NOC) utilizes its own intranet webpage dedicated to its policies and procedures. Content is updated in real time on the intranet webpage to ensure NOC employees are always aware of the newest policy or procedures. On an annual basis, NOC management performs a review of information on the NOC intranet webpage to ensure the information is up-to-date and accurate.

The NOC utilizes a ticketing system to track all incidents and customer requests. On a monthly basis, ticket resolution metrics are prepared and presented to Operations Management. Each customer in Internap data centers is given a Service Level Agreement (SLA) and Customer Colocation Handbook with all necessary customer facing information and procedures to follow for many common questions/requests, such as system availability issues and what to do when a possible security breach is identified, along with many other incident responses. The information in the Customer Colocation Handbook is reviewed on an annual basis by data center management to ensure the information is up-to-date and accurate. Additionally, Internap customers connect to Internap via the Internap website and online customer portal. The Internap website hosts a detailed description of Internap data center services and the portal houses customer specific information and enables customers to contact Internap directly through the system. This customer portal, along with ad hoc communication methods are utilized to ensure transparent communication with customers. The description of Internap data center operations can be broken down into the specific components of infrastructure, monitoring, people and security software components.

Infrastructure, Environmental and System Monitoring Components:

Internap's data center operations consist of a strong physical infrastructure, including secure facilities featuring N+1 redundancy for both power and cooling, along with fire protection and system monitoring. The existing facility and environmental standards at the data centers are designed to ensure that uptime is maximized by providing redundancy to key facility and environmental systems to ensure that mechanical or electrical failures will not result in an outage.

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

Monitoring Environmental Conditions and Critical Work Authorizations
Data center environmental conditions are constantly monitored and reported via an automated Building Management System (BMS). Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor a BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. If any issues or incidents with these environmental systems arise, the console displays an alert and e-mails on-site data center personnel.

Internap has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our customers. Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are re-visited annually by Internap data center and operations management to assess the risk associated with the threats identified.

Smoke/Fire Detection
The smoke/fire detection system in the data centers comprises smoke detectors and either a particulate sampling system or a very early smoke detection apparatus (VESDA) system that detects smoke during the very early stages of combustion. The smoke detection system is the first line of defense against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room, and the BMS generates console and e-mail alerts to data center employees.

The smoke detection system is inspected and serviced at least annually to ensure effective operation.

Fire Suppression
The fire suppression system consists of a pre-action dry pipe system. The pre-action dry pipe system is designed to keep water out of the sprinkler system plumbing in the data center areas during normal operations. If smoke and/or excessive heat is detected, and a sprinkler fusible head melts as a result, water is pumped into the sprinkler systems for the affected zone(s) only. The BMS continuously monitors and reports the status of the fire suppression system.

The fire suppression systems are inspected and serviced at least annually to ensure effective operation. Clean agent fire extinguishers are also provided throughout the data center for accessibility in the event of a fire within the data center (or elsewhere in the building).

Fire extinguishers are inspected and serviced at least annually to ensure effective operation.

Heating, Ventilation, and Air Conditioning (HVAC)
Multiple HVAC units control both temperature and humidity within the data center and are configured in a redundant formation to ensure operation continues if a unit fails. Temperature and humidity are maintained to current SLA standards. The HVAC units are monitored by the BMS within the facility control room and NOC.

HVAC units are inspected and serviced at least annually to ensure effective operation.

Utility Power and Backup Power Systems
The data center is supplied by power feeds from the servicing utility to support daily operations. The power feeds are channeled into redundant UPS systems which condition the power to be supplied to data center equipment. These redundant UPS units allow customers to opt for redundant N+1 power feeds to their equipment.

In the event of a utility power outage, the UPS system automatically switches to backup power from a battery farm which supplies power for 15 to 20 minutes until multiple diesel generators power up. Internap maintains a sufficient on-site fuel reserve, which gives the generators capability to power the data center for at least 24 hours. Each of Internap's Company controlled facilities maintain contracts with fuel companies for the delivery of fuel as needed.

The UPS systems and generators are inspected and serviced at least annually to ensure effective operation.

Personnel, Security and Software System Components

Internap's commitment to competence includes management's determination of the levels of competence and expertise required for each position in the data centers, ensuring highly technical and customer service focused data center employees. Internap provides 24/7 manned facilities with a host of security features designed to protect our customer's equipment and network connectivity. Internap controls ingress and egress using electronic keycard and/or biometric software. All cages and cabinets are securely locked and CCTV monitors and records activity within each facility.

Organizational Structure and Assignment of Authority and Responsibility

Internap has developed an organizational structure that adequately suits the nature and scope of our operations. The Company has developed organizational charts that internally convey employee reporting relationships, operational responsibilities, and the overall organizational hierarchy.

Human Resource Policies and Practices

Internap's human resource department has policies and established practices that govern the hiring, termination, evaluation, promotion, counseling, and compensation of current and prospective company employees. A documented set of human resource, operational, and financial policies and procedures, along with a complete list of internal controls are made available to applicable employees via the intranet. Internap HR personnel prepare detailed job descriptions and organizational charts that capture and convey these requirements for each position. Internap also facilitates employee development through annual evaluations, on-site training, a company-wide tuition reimbursement program, and the allocation of funds for relevant off-site training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with Internap. Newly hired data center employees receive training and are made aware of customer facing documents and other internal policies covering system security and availability. For terminated employees, Internap has a formal process for decommissioning access to company records and systems in a timely manner.

Security Staff

A contracted security company employs and provides Internap's data center security resources. Such outsourcing ensures consistency of training, performance, metrics, and supervision. Responsibilities of security include, but are not limited to the following.

- Monitoring of Physical Security Systems
- Monitoring of Physical Security Standards
- Loss Prevention
- Internal Investigations
- Security Policies and Procedures Compliance

Security Control Desk

All Internap data centers have a Security Control Desk to control access, monitor security alarms, monitor Closed-Circuit Television camera signals (CCTV), and support security-related operational activities

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

24/7/365. Security personnel are on-site 24 hours a day, 7 days a week, 365 days a year. The Security Control Desk possesses the following.

- Central ventilation, heating & air conditioning
- Real-time monitoring of data center door alarms
- Real-time monitoring of data center CCTV cameras
- Centralized security service and emergency dispatch communications for Security Staff, as well as for local fire departments, police departments, and other emergency response resources
- Electrical power support for continuous operation of communications, lighting, CCTV, intrusion detection, and alarm monitoring equipment in the event of utility power loss

Access Control

Internap employs a computerized Access Control System (ACS) to control physical access to our data centers that house customer equipment, media and documentation. The ACS utilizes proximity card readers with pin codes or biometrics to control access into perimeter doors, shipping & receiving areas, storerooms, and other critical areas. In 2013, Internap upgraded the ACS to the most current version. This required a migration to new hardware and software to support the updated application. Customers and employees (including contractors and security guards) must follow formal access request and approval processes before physical access to our data centers is granted. Additional access control features are as follows.

- Access to the data center and other restricted areas is specifically limited to authorized individuals
- Internap access badges with pin codes or biometrics are required to gain entry to critical areas.
- Customers, Vendors, Contractors and other Visitors must be sponsored by an Internap-approved host to gain access if not on the Customer-Approved List
- All Customers, Vendors, Contractors (non-security guards), and Visitors on the Customer-Approved List must check in with the Security Desk upon arrival with a photo identification if they require the physical key to access cages. Those customers with badge cage access will have automatic access to their cages.
- Visitors and others not on the Customer-Approved List are escorted while in the data center and other critical areas
- Guest access for approved Contractors is generally limited to particular areas where work is being performed. Long term contractors are granted more general access via personal badges.
- Employees with access to the data center are limited to those with a specific business need or job function.

Administrator access (add, modify and delete users) in the SEF is restricted to appropriate personnel based on job roles and responsibilities and reviewed during periodic access reviews. Data Center Management authorizes Administrator access to the keycard system based on the individuals' job responsibilities.

The SEF is also used to monitor, notify, and log security alarms. The system monitors:

- Perimeter/external doors
- Restricted area doors
- Data center doors
- Shipping/receiving doors

SEF is equipped and programmed to receive alarms for forced doors, propped doors, and denied card read attempts.

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

Visitor/Sales Tour Access
All Internap data center tours must be coordinated with an Internap representative. Tours of the data center and other restricted areas require an escort from an authorized Internap employee.

Customer Access
Each customer is permitted to designate individuals with access to Internap data centers via the Network Operations Center (NOC). The customers make requests for access through the NOC via email, phone call, or the online Customer Portal. The NOC manages customers' respective Customer Access Lists (CAL) within the newly designed Ubersmith Facility Management application, which went live in July 2013, replacing the Colo-Space Tracker (CST) application, which was in place prior to the Ubersmith implementation. Update access to the CAL is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to the CALs and will only allow individuals listed on a Company's CAL access to the data center. The customer is responsible for requesting additions, modification, or deletions to access; the NOC is responsible for management of the Customer Access List. Upon notification of a customer employee termination or revocation of customer agreement, physical access to the data center is revoked. Customers are responsible for retaining a terminated employees access badge and either destroying it or returning it to Internap security.

Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.

Cages are secured via one of two possible means: 1) physical key; and 2) badge.

1) physical key - Keys are maintained by Internap security personnel. After the security personnel determine appropriate authority per the Customer Access List, they escort the customer to the cage and unlock it for them; or

2) badge access - access is controlled via the SEF similar to that of data center access.

Cabinets are secured via one of two possible means: 1) physical key; or 2) combination.

1) physical key - Keys are maintained by Internap security personnel. After the security personnel determine appropriate authority per the Customer Access List, they escort the customer to the cabinet and unlock it for them; or

2) combination - access is controlled via the use of a customer specific combination code.

Customer and Employee Access Review
Internap data center security personnel perform a semi-annual audit to validate the appropriateness of all customer employees' physical access to the data centers. Internap data center security personnel perform a quarterly audit to validate the appropriateness of all employees', contractors', and security guards' physical access to the data centers. As part of a semi-annual audit, individuals with access to add, modify, and delete users in the key card system are reviewed for appropriateness.

Data Center Check-In Process

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

1. Identify—upon request for access, the security officer on duty will identify the type of requestor (Customer, Visitor, Contractor, or Internap employee without continuous access).
2. Verify— the security officer will reference the Customer Access List to ensure that the individual(s) requesting access is (are) authorized. If the individual(s) is (are) not on the listing, a ticket is initiated by the Network Operations Center (NOC) requesting access to the data center from an authorized Customer administrator on the CAL. Authorization must be documented within the ticket before access is granted.
3. Review—Security requires that each individual entering the data center (outside of authorized Internap employees, contractor or security guards and customers with continuous access) present a valid photo ID prior to gaining access.
4. Access—once the information is verified by security, a temporary access card for the authorized areas will be programmed by security.

Employee and Security Guard Access to Data Center
Access to the data center is restricted to only those Internap employees with a legitimate business need. Access, if temporarily required for other employees whose job functions do not necessitate access to the data center on a day-to-day basis, is granted on a case-by-case basis by the data center manager, and these employees must be escorted by data center personnel. Physical access to the data center is revoked upon termination of Internap employees, and security guards.

Contractor and Vendor Access to Data Center
Access to the data center is restricted to Contractors and Vendors with a legitimate business purpose. Access is granted with a daily temporary badge and logged with security unless the Contractor or Vendor will be on site for an extended period of time or multiple times over an extended period (i.e. multiple weeks). Data Center management will notify Security of an expected Contractor or Vendor, and if a Contractor or Vendor arrives unexpectedly, Security will contact Data Center management to gain approval for temporary access. Temporary access cards are returned to security prior to leaving our facilities. If a temporary badge is not returned at the end of the day, it is disabled in the system by Security. Physical access to the data center is revoked upon completion of the contractors' and/or vendors' duties.

General Visitor Rules

1. All visitors must be escorted at all times by an authorized host or employee.
2. Internap data center regulations must be strictly followed at all times. Any individual (including Internap employees) not adhering to these rules will be escorted from the data center by staff and/or security.

Surveillance and Monitoring

1. Internap data centers employ a CCTV (Closed Circuit Television) to record and facilitate monitoring of the data center. Cameras are positioned to provide views of critical areas, including perimeter doors, main entrances and exits, shipping & receiving, and other areas of importance.
2. Internap security desk personnel monitor the signals from the CCTV system. The desk is connected by secure cables to the cameras throughout the facility to permit both interior and exterior surveillance.
3. Camera images are recorded on site via digital video recorders 24/7/365. These visual records are retained for at least 30 days to provide details of activity at Internap data centers.
4. Internap provides dedicated 24/7/365 CPS (continuous power supply) and standby emergency power via generator to support security systems.

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

System boundaries

Internap's data center operations, as described above, address all of the applicable Trust Services criteria related to the Availability principle, with the exception of the following criteria that are not applicable to Internap's data center operations model:

3.4 - Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.

3.7 - Procedures exist to protect against unauthorized access to system resources (specifically perimeter network security, remote access, and the like).

3.8 - Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.

3.9 - Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

3. 11 - Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.15 - Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.

Additionally, components of other applicable Trust Services criteria related to the Availability principle associated with backups, access to system resources and configurations, network management and protection, virus protection, encryption, and data are not applicable to Internap's data center operations.

Each of the six criteria noted above is classified under Internap's complementary user-entity control considerations, as Internap is responsible for providing a safe, secure, environmentally stable facility with uninterruptable power and internet connectivity for our customers to house their network equipment. Customers are responsible for protecting their network and data on the equipment they house in Internap's data centers.

Section III: Description of the Internap Network Services Corporation's SEF Company-Controlled Data Center System

Complementary User-Entity Controls

Internap's services are designed with the assumption that certain controls will be implemented by user organizations. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain Availability Trust Services Criteria included in this report. The following is a representative list of controls that are expected to be in operation at user organizations to complement the controls of Internap; this is not a comprehensive list of all controls that should be employed by our user organizations.

1. User organizations are responsible for understanding and complying with their contractual obligations. (all criteria)
2. User organizations are responsible for ensuring the supervision, management, and control of the use of Internap's services by their personnel. (all criteria)
3. User organizations are responsible for designating authorized individuals for access requests to Internap's data center. (criterion 3.6)
4. User organizations are responsible for notifying Internap of terminated employees. (criterion 3.6)
5. User organizations are responsible for retaining a terminated employee's access badge and either destroying it or returning it to Internap security. (criterion 3.6)
6. User organizations are responsible for changing their cabinet combination lock password after individuals with knowledge of the current combination are terminated. (criterion 3.6)
7. User organizations are responsible for periodically reviewing their Customer Access Lists. (criterion 3.6)
8. User organizations are responsible for immediately notifying Internap of any actual or suspected information security breaches, including compromised user accounts. (criterion 3.6)
9. User organizations are responsible for notifying Internap of changes made to technical or administrative contact information. (criterion 3.6)
10. User organizations are responsible for applying logical access security controls, data encryption controls, and related procedures to their network connected equipment. (criteria 3.7, 3.9)
11. User organizations are responsible for the logical protection of their data, including performing backup procedures and classification procedures as necessary. (criteria 3.4, 3.7, 3.11)
12. User organizations are responsible for protecting their equipment against infection by computer viruses, malicious codes and unauthorized software. (criterion 3.8)
13. User organizations are responsible for maintaining their own system components and configurations. (criterion 3.15)
14. User organizations are responsible for protecting and maintaining the security of system resources (e.g., secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services). (criterion 3.15)
15. User organizations are responsible for notifying Internap of any system availability issues. (criterion 2.2)

The trust services criteria and the related controls that meet the criteria are listed in the accompanying section IV of this report, "Internap's Control Activities and PwC's Tests of Controls"

Section IV: Internap's Control Activities and PwC’s Tests of Controls

Introduction

PwC tested relevant aspects of Internap Network Services Corporation's ("the Company") control environment and the controls specified on the following pages. PwC's tests covered only those controls provided by the Company and did not cover controls which may be specific to individual customers of the Company.

Control Objective 1: Policies

The entity defines and documents its policies for the availability of its system.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
1.1	The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	A - A written Data Center Operations Manual, Customer Colocation Handbook, and Network Operations Center Procedures are in place documenting data center policies and procedures.	**Inspection** Inspected the manuals to determine whether availability and security policies and procedures are documented within.	No exceptions noted.
		B - The Data Center Operations Manual is reviewed and approved by the Data Center Operations management on an annual basis.	**Inspection** Inspected the Data Center Operations Manual to determine whether it is reviewed and approved by Data Center Operations management on an annual basis.	No exceptions noted.
		C - The Network Operations Center procedures are reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	**Inspection** Inspected the Network Operations Center procedures to determine whether they were reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	No exceptions noted.
		D - The customer Colocation Handbook is reviewed and approved by the Colocation business unit management on an annual basis.	**Inspection** Inspected the Customer Colocation Handbook to determine whether it is reviewed and approved by business unit management on an annual basis.	No exceptions noted.

Section IV: Internap's Control Activities and PwC's Tests of Controls

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
1.2	The entity's system availability and related security policies include, but may not be limited to, the following matters. a. Identifying and documenting the system availability and related security requirements of authorized users. b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements c. Assessing risks on a periodic basis d. Preventing unauthorized access. e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access. f. Assigning responsibility and accountability for system availability and related security. g. Assigning responsibility and accountability for system changes	A - A written Data Center Operations Manual, Customer Colocation Handbook, and Network Operations Center Procedures are in place documenting data center policies and procedures.	**Inspection** Inspected the manuals to determine whether availability and security policies and procedures are documented within.	No exceptions noted.
		B - The Data Center Operations Manual is reviewed and approved by the Data Center Operations management on an annual basis.	**Inspection** Inspected the Data Center Operations Manual to determine whether it is reviewed and approved by Data Center Operations management on an annual basis.	No exceptions noted.
		C - The Network Operations Center procedures are reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	**Inspection** Inspected the Network Operations Center procedures to determine whether they were reviewed and approved by the Network Operations Center (NOC) management on an annual basis.	No exceptions noted.
		D - The customer Colocation Handbook is reviewed and approved by the Colocation business unit management on an annual basis.	**Inspection** Inspected the Customer Colocation Handbook to determine whether it is reviewed and approved by business unit management on an annual basis.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	and maintenance. h. Testing, evaluating, and authorizing system components before implementation. i. Addressing how complaints and requests relating to system availability and related security issues are resolved. j. Identifying and mitigating system availability and related security breaches and other incidents. k. Providing for training and other resources to support its system availability and related security policies. l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies. m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service level agreements, and other contractual requirements. n. Recovering and continuing service in accordance with documented customer commitments or other agreements. o. Monitoring system capacity to achieve customer commitments or	G - Users (customers) are given a "colocation handbook" and receive a Service Level Agreement when they sign up to use our services.	**Inquiry** Inquired of Internap personnel to determine whether new colocation customers are provided the Colocation Handbook and Service Level Agreement upon initiating service. **Inspection** Inspected the Colocation Handbook and a sample of Service Level Agreements to determine whether they exist and include related availability and security obligations of users and Internap's availability and security commitments. **Inspection** Inspected the customer set up checklist to determine whether procedures exist to instruct the business to provide the Colocation Handbook and Service Level Agreement to new customers.	No exceptions noted.
		L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been reviewed and risks assessed between October 1, 2012 and September 30, 2013.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	other agreements regarding availability	M - The Company performs an enterprise wide risk assessment annually.	**Inspection** Inspected documentation to determine whether an enterprise wide risk assessment was completed and reviewed between October 1, 2012 and September 30, 2013.	No exceptions noted.
1.3	Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.	E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry** Inquired of management to determine whether the organizational chart and job descriptions are updated at least annually. **Inspection** Inspected the Internap Organizational chart and job descriptions to determine whether the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.

Area 2: Communications

The entity communicates the defined system availability policies to responsible parties and authorized.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	F - The Company has prepared a description of its colocation service offerings and posts it to the Company website for users to access.	**Observation** Observed Internap’s external website to determine whether a description of its colocation service offerings and system boundaries are posted.	No exceptions noted.
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	F - The Company has prepared a description of its colocation service offerings and posts it to the Company website for users to access.	**Observation** Observed Internap's external website to determine whether a description of its colocation service offerings and system boundaries are posted.	No exceptions noted.
		G - Users (customers) are given a "colocation handbook" and receive a Service Level Agreement when they sign up to use our services.	**Inquiry** Inquired of Internap personnel to determine whether new colocation customers are provided the Colocation Handbook and Service Level Agreement upon initiating service. **Inspection** Inspected the Colocation Handbook and a sample of Service Level Agreements to determine whether they exist and include related availability and security obligations of users and Internap's availability and security commitments. **Inspection** Inspected the customer set up	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			checklist to determine whether procedures exist to instruct the business to provide the Colocation Handbook and Service Level Agreement to new customers.	
		H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. **Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection** Inspected the Data Center Operations Manual to determine whether it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
2.3	Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry** Inquired of management to determine whether the organizational chart and job descriptions are updated at least annually. **Inspection** Inspected the Internap Organizational chart and job descriptions to determine whether the company assigned responsibility and accountability for system availability and security.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.4	The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. **Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection** Inspected the Data Center Operations Manual to determine whether it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
		J - The process for users (customers) to inform the entity of system availability issues, possible security breaches, and other incidents is documented in the "customer handbook".	**Inspection** Inspected the Customer Handbook to determine whether the process for customers to inform Internap of system availability issues, possible security breaches, and other incidents was documented.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
		K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to customers.	**Inspection** For a sample of data center changes between October 1, 2012 and September 30, 2013, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.

Area 3: Procedures

The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been reviewed and risks assessed between October 1, 2012 and September 30, 2013.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inspection** Inspected documentation to determine whether an enterprise wide risk assessment was completed and reviewed between October 1, 2012 and September 30, 2013.	No exceptions noted.
3.2	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	N - A VESDA or particulate sampling smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire at its very early stages.	**Observation** Observed the smoke detection system in the data center to determine whether a smoke detection system is installed in the data center.	No exceptions noted.
		O - The VESDA or particulate sampling smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether the smoke detection system is inspected and serviced between October 1, 2012 and September 30, 2013.	No exceptions noted

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		P - The data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system as well as fire extinguishers located throughout the data center.	**Observation** Observed sprinkler system and fire extinguishers throughout the data center to determine whether the data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system as well as fire extinguishers.	No exceptions noted.
		Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between October 1, 2012 and September 30, 2013.	No exceptions noted
		R - Multiple HVAC units control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	**Observation** Observed multiple HVAC units to determine whether HVAC units are designed to control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		S - HVAC units are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether HVAC units are inspected and serviced annually during the period.	No exceptions noted.
		K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes that occurred between October 1, 2012 and September 30, 2013, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.
		T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to determine whether redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
		U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether UPS systems are inspected and serviced at least annually during the period.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to determine whether multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
		W - Generators are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether generators are inspected and serviced at least annually during the period	No exceptions noted.
		X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	
3.3	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to determine whether redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
		V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to determine whether multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
3.5	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: a. Logical access security measures to restrict access to information resources not deemed to be public. b. Identification and authentication of users. c. Registration and authorization of new users. d. The process to make changes	Y - Data Center Management approves all provisioning of Administrator access (add, modify, delete users) to the keycard system.	**Inspection** Inspected a sample of administrative users added between October 1, 2012 and September 30, 2013 to determine whether access was approved by Data Center Management.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	and updates to user profiles. e. Restriction of access to offline storage, backup data, systems and media. f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	Z - On a semi-annual basis, individuals with access to add, modify, and delete users in the key card system are reviewed for appropriateness.	**Inspection** Inspected the semi-annual access review to determine whether Internap collocation security personnel perform a semi-annual access review to validate the appropriateness of individuals with access to add, modify, and delete users in the key card access system and access changes requested were implemented.	No exceptions noted.
		AA - User update access to CST and Ubersmith customer contact lists is reviewed for appropriateness based on job responsibilities on an annual basis.	**Inspection** Inspected the review of update access to the CST/Ubersmith customer contact lists to determine whether access is limited to authorized personnel only.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		OO - Internap colocation security personnel perform a quarterly audit to validate the appropriateness of all employees', contractors', and security guards' physical access to the data centers.	**Inspection** Inspected a sample of quarterly audits of employees, contractors, and security guards with data center access to determine whether the reviews were performed and access changes requested were implemented.	No exceptions noted.
		PP – Data Center Operation’s application data migrations are reconciled to validate the completeness and accuracy the migrated data.	**Inspection** Inspected the reconciliations performed by Internap management to determine whether user access listing reconciliations were performed between the legacy and newly implemented Access Control System (ACS) and between CST and the Ubersmith application.	**Exceptions noted.** Design Deficiency: There was not a control designed to reconcile user access data migrated as part of the Access Control System (ACS) migration.
3.6	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	BB - Only authorized Internap employees, contractors, security guards, and customers are granted physical access to the data center.	**Inspection** Inspected authorization evidence for a sample of employees, contractors, customers and security guards, who were granted physical access to the data center between October 1, 2012 and September 30, 2013 to determine whether only	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			authorized Internap employees and customers are granted physical access to the data center.	
		CC – 1 - Physical access to the data center is revoked upon termination of Internap employees and security guards.	**Inspection** Inspected the active keycard listing for a sample of terminated employees and security guards to determine whether physical access to the data center is revoked upon termination of Internap employees and security guards.	No exceptions noted.
		CC-2-Physical access to the data center is revoked upon termination of contractors.	**Inquiry** Inquired of data center management to determine whether physical access to the data center is revoked upon termination of contractors.	**Exceptions noted.** No auditable evidence was retained to evidence the removal of contractor badge access to the data center environment.
		DD - Physical access to the data center is revoked upon notification by customers to the NOC for customer employee terminations.	**Inspection** For a sample of customer employees who require data center access revocation, inspected the keycard access listings to determine whether unauthorized the customer employee access had been removed.	No exceptions noted.
		EE - Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.	**Inquiry** Inquired of data center management to determine whether customer equipment is segregated via locked cages	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		Physical keys are maintained by the security guard and stored out of plain sight.	or locked cabinets to ensure that customers can only access their own equipment. **Observation** Observed locked cages and locked cabinets to determine whether customer equipment is segregated via locked cages or locked cabinets such that customers can only access their own equipment. **Observation** Observed that physical keys are maintained by the security guards and stored out of plain sight.	
		FF - In order to gain physical access to Internap data centers, employees and customers must be validated via a combination of key card and/or biometric technology.	**Inquiry** Inquired of management to determine whether employees and customers must be validated by key card and/or biometric technology. **Observation** Observed successful and unsuccessful attempts to gain entry to the data center to determine whether employees and customers must be validated by keycard and/or biometric technology.	No exceptions noted.
		GG - A manned security post controls entry into Internap data centers. Customers must pass by the manned security post prior to gaining access to the data center.	**Inquiry** Inquired of data center management to determine whether a manned security post controls entry into	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Internap data centers. **Observation** Observed the manned security post that is placed in line of sight to where customers gain access to the data center to determine whether a manned security post controls entry into Internap data centers.	
		JJ - Internap employs 24 hour video surveillance to monitor all entrances, exits, and other sensitive areas of its data centers.	**Observation** Observed video surveillance cameras at entrances, exits, and sensitive areas as well as security personnel monitoring video feeds to determine whether sensitive locations are monitored by Internap personnel.	No exceptions noted.
		HH - Customer access to Internap data centers is logged at the security desk.	**Inspection** Inspected security logs for a sample of days to determine whether customer access to Internap data centers is logged at the security desk.	No exceptions noted.
		OO - Internap colocation security personnel perform a quarterly audit to validate the appropriateness of all employees', contractors', and security guards' physical access to the data centers.	**Inspection** Inspected a sample of quarterly audits of employees, contractors, and security guards with data center access to determine whether the reviews were performed and access changes requested were implemented.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		PP – Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy the migrated data.	**Inspection** Inspected the reconciliations performed by Internap management to determine whether user access listing reconciliations were performed between the legacy and newly implemented Access Control System (ACS) and between CST and the Ubersmith application.	**Exceptions noted.** Design Deficiency: There was not a control designed to reconcile user access data migrated as part of the Access Control System (ACS) migration.
		II - Internap colocation security personnel perform a semi-annual audit to validate the appropriateness of all customers' physical access to the data centers.	**Inspection** Inspected the semi-annual customer audits to determine whether Internap collocation security personnel perform a semi-annual audit to validate the appropriateness of customers' physical access to the data centers.	No exceptions noted.
3.10	Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	H - Internal Users (employees) receive on the job new hire training and are made aware of the customer facing documents and other internal policies covering system security and availability.	**Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are provided on the job training. **Inquiry** Inquired of Data Center Operations management to determine whether new colocation employees are made aware of customer facing documents and internal policies addressing data center security and availability. **Inspection**	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Inspected the Data Center Operations Manual to determine whether it contains information to be leveraged in the training of internal users. Such information includes instructions for informing user entities about system availability issues, breaches of system security, and submitting complaints.	
		I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.12	Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	O - The VESDA or particulate sampling smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether the smoke detection system is inspected and serviced between October 1, 2012 and September 30, 2013.	No exceptions noted
		Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between October 1, 2012 and September 30, 2013.	No exceptions noted
		S - HVAC units are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether HVAC units are inspected and serviced annually during the period.	No exceptions noted.
		U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether UPS systems are inspected and serviced at least annually during the period.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		W - Generators are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether generators are inspected and serviced at least annually during the period.	No exceptions noted.
		X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC)	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	
		L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been reviewed and risks assessed between October 1, 2012 and September 30, 2013.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inspection** Inspected documentation to determine whether an Enterprise Wide Risk Assessment was completed and reviewed between October 1, 2012 and September 30, 2013.	No exceptions noted.
		KK - Issue tracking tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether issue tracking tickets resolution metrics are reported to operations management monthly to monitor the timeliness of completion. **Inspection** For a sample of months inspected the operations management reporting package to determine whether ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.13	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes between October 1, 2012 and September 30, 2013, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.
3.14	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.	LL - An employment pre-screening process is in place. It includes background, credit, and DMV checks (based on job requirements).	**Inspection** Inspected pre-screen results in the employee files for a sample of employees hired between October 1, 2012 and September 30, 2013 to determine whether an employment pre-screening process is in place and includes background, credit and DMV checks where applicable based on job requirements.	No exceptions noted.
		MM - An annual performance review process is in place. It gives managers and employees an opportunity to discuss performance, ethics, integrity and training needs. The review process also includes setting goals and objectives for the following year.	**Inspection** Inspected documentation evidencing the annual performance review process is in place and discusses ethics, integrity, training needs, along with setting goals for the upcoming year.	No exceptions noted.
		E - Organizational chart and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inspection** Inspected the Internap Organizational chart and job descriptions to determine whether the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		NN - The Company allows operating units to budget training for each employee to continue education either virtually or locally, including maintenance of certifications. The Company also has a formal tuition reimbursement program.	**Inspection** Inspected the Employee Handbook and annual budget to determine whether the Company allows operating units to budget training for each employee to continue education either virtually or locally, including maintenance of certifications and whether the Company also has a formal tuition reimbursement program. **Inspection** Inspected Internap's operating budget for 2013 to determine whether it included allowance for training and continuing education.	No exceptions noted.
3.16	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes between October 1, 2012 and September 30, 2013, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
3.17	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	I - Each Internap Company controlled data center has an Operations Manual which is available and communicated to users (emergency procedures are documented within).	**Inspection** Inspected the Operations Manual to determine whether it contained relevant content including: Emergency and Incident Response; Authorized Vendors; Facility Map with Equipment Location; Equipment Descriptions; Equipment Specifications; Facility Capacities; Preventive Maintenance; Trouble Ticket and Engineer Change Notice (ECN) Procedures; Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	No exceptions noted.
		K - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are documented and authorized to ensure minimal impact to our Customers.	**Inspection** For a sample of data center changes between October 1, 2012 and September 30, 2013, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.

Area 4: Monitoring

The entity monitors the system and takes action to maintain compliance with its defined system availability policies.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4.1	The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			conditions.	
		KK - Tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether tickets resolution metrics are reported to operations management monthly to monitor the timeliness of completion. **Inspection** For a sample of months inspected the operations management reporting package to determine whether ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		N - A VESDA or particulate sampling smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire at its very early stages.	**Observation** Observed the smoke detection system in the data center to determine whether a smoke detection system is installed in the data center.	No exceptions noted.
		O - The VESDA or particulate sampling smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether the smoke detection system is inspected and serviced between October 1, 2012 and September 30, 2013.	No exceptions noted
		L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been reviewed and risks assessed between October 1, 2012 and September 30, 2013.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		M - The Company performs an enterprise wide risk assessment annually.	**Inspection** Inspected documentation to determine whether an Enterprise Wide Risk Assessment was completed and reviewed between October 1, 2012 and September 30, 2013.	No exceptions noted.
		P - The data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system as well as fire extinguishers located throughout the data center.	**Observation** Observed sprinkler system and fire extinguishers throughout the data center to determine whether the data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system as well as fire extinguishers.	No exceptions noted.
		Q - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between October 1, 2012 and September 30, 2013	No exceptions noted .
		R - Multiple HVAC units control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	**Observation** Observed multiple HVAC units to determine whether HVAC units are designed to control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		S - HVAC units are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether HVAC units are inspected and serviced annually during the period.	No exceptions noted.
		T - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Observation** Observed UPS systems to determine whether redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
		U - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inspection** Inspected a third-party vendor preventative maintenance and inspection report to determine whether UPS systems are inspected and serviced at least annually during the period.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		V - Multiple diesel generators are in place to provide backup power in the event of a power outage.	**Observation** Observed generators to determine whether multiple diesel generators are in place to provide backup power in the event of a power outage.	No exceptions noted.
		W - Generators are inspected and serviced at least annually by third party vendors to ensure effective operation.	**Inspection** Inspected a sample of third-party vendor preventative maintenance and inspection reports to determine whether generators are inspected and serviced at least annually during the period.	No exceptions noted.
		KK - Tickets resolution metrics are reported to Operations management monthly to monitor the timeliness of completion.	**Inquiry** Inquired of operations management to determine whether tickets resolution metrics are reported to operations management monthly to monitor the timeliness of completion. **Inspection** For a sample of months inspected the operations management reporting package to determine whether ticket resolution metrics were included and monitored for timeliness of completion.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
4.3	Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.	X - Data center environmental conditions are monitored and reported via the BMS. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	**Inquiry** Inquired of data center management to determine whether data center environmental conditions are monitored and reported via the BMS and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions. **Observation** Observed the local control room at the data center and Internap's centralized Network Operations Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the BMS. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BMS console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		L - Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually to assess the risk associated with the threats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been reviewed and risks assessed between October 1, 2012 and September 30, 2013.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inspection** Inspected documentation to determine whether an Enterprise Wide Risk Assessment was completed and reviewed between October 1, 2012 and September 30, 2013	No exceptions noted.

Section V: Other Information Provided by Internap Management

Ref. #	Control Activity	PwC Findings	Management Response
1	PP – Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy the migrated data.	**Exceptions noted.** Design Deficiency: There was not a control designed to reconcile user access data migrated as part of the Access Control System (ACS) migration.	In 2013 Internap initiated a project to upgrade our Access Control System for our company-controlled data centers. This project scope involved updating both hardware and software to achieve a state-of-the-art automated security system with much greater functionality and reporting capabilities. Although we engaged a third party technical service provider to lead our system upgrade, the appropriate quality control measures were not put in place to ensure the data migration integrity. During the annual audit process, we identified that at certain data centers, a time gap of between four and six weeks occurred in the information migrated from the old system to the new system. Upon identification of this issue, we immediately reconciled and corrected the data, as well as remediated the gap by creating a new control procedure to ensure this would not happen for subsequent conversions. Our new control states, "Data Center Operation's application data migrations are reconciled to validate the completeness and accuracy the migrated data." This reconciliation will take place for the remaining data center migrations. Although a time gap occurred, it is important to note that the conversion did not result in any inappropriate access to our data centers or cause any security incidents. All of our other security controls operated as designed, providing our customers with a safe, secure environment throughout the period. As stated above, we have remediated this issue to ensure there is no data integrity gap. We plan to undergo another SOC 2 audit as soon as possible to show our customers our commitment to operating excellence.