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 April 1, 2011 - September 30, 2011

Table of Contents

SECTION I: REPORT OF INDEPENDENT SERVICE AUDITORS **3**

SECTION II: MANAGEMENT OF INTERNAP NETWORK SERVICES CORPORATION'S ASSERTION **5**

SECTION III: DESCRIPTION OF THE INTERNAP NETWORK SERVICES CORPORATION'S SEF COMPANY-CONTROLLED DATA CENTER SYSTEM **7**

SECTION IV: DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF **17**

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 for the Period April 1, 2011, to September 30, 2011" (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 April 1, 2011, to September 30, 2011. 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 for the Period April 1, 2011, to September 30, 2011", which is based on the criteria identified in 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; and (5) 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 April 1, 2011, to September 30, 2011.

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

Section I: Report of Independent Service Auditors

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.

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 system that was designed and implemented throughout the period April 1, 2011, to September 30, 2011.
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 April 1, 2011 to September 30, 2011, and user entities applied the complementary user-entity controls contemplated in the design of Internap Network Services Corporation's controls throughout the period April 1, 2011, to September 30, 2011.
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 April 1, 2011, to September 30, 2011.

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 "Description of Test of Controls and Results Thereof."

Intended 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 April 1, 2011, to September 30, 2011; independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, 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.

PricewaterhouseCoopers LLP

Atlanta, GA
December 7, 2011

INTERNAP®

Section II: Management of Internap Network Services Corporation's Assertion

We have prepared the attached description titled "Description of Internap Network Services Corporation's SEF Company-Controlled Data Center System for the Period April 1, 2011, to September 30, 2011" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.33–.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the 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 April 1, 2011 to September 30, 2011, based on the following description criteria:

   i. The description contains the following information:

      1. The types of services provided

      2. The components of the system used to provide the services, which are the following:

         - Infrastructure - The physical and hardware components of a system (facilities and equipment).

         - Software - The programs used to manage active customers and data center badge access.

         - People - The personnel involved in the operation and use of a system (operators, users, and managers).

         - 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 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

INTERNAP®

Section II: Management of Internap Network Services Corporation's Assertion

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. the controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

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

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

Company Background

Internap Network Services Corporation (NASDAQ: INAP) is an Internet solutions and data center company providing a suite of network optimization and delivery services and products that manage, deliver and distribute applications and content with a 100% availability service level agreement, as well as a global provider of secure and reliable data center services. Internap helps our customers innovate, improve service levels and lower the cost of information technology operations. Internap's services and products, combined with progressive and proactive technical support, enable our customers to migrate business-critical applications from private to public networks.

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 operations, which primarily include physical space for hosting customers' network and other equipment plus associated services such as redundant power and network connectivity, 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 ten company-controlled facilities for which SOC 2-Availability examinations are performed and 27 partner sites. 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 one of our ten company-controlled data center facilities for which SOC 2-Availability examinations are performed specific to the Availability principle set forth in TSP section 100, *Trust Service Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy*.

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.

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 annual Sarbanes-Oxley assessment procedures and other 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 over financial reporting or specific testing procedures. Any deficiencies in the Company's system of internal control 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.

This report is intended solely for the use by the management of Internap, its 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.

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

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 these 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 our data centers is given a 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, our customers connect to us via our 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 us directly through the system. This customer portal, along with ad hoc communication methods are utilized to ensure transparent communication with customers.

The description of our data center operations can be broken down into the specific components of Infrastructure, Software, People, and Procedures.

This report is intended solely for the use by the management of Internap, its 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.

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

Infrastructure, Environmental and System Monitoring Components:

Internap's data center operations consist of a strong physical infrastructure, including secure facilities, located in major metropolitan areas, 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 center 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 the Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor a BACtalk 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 our data centers is comprised of 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 defence against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room and the BACtalk system 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 Alerton Envision BACtalk system 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 is maintained between

64 and 78 degrees, with humidity maintained between 30 and 70 percent. The HVAC units are monitored by the Alerton Envision BACtalk system within the facility control room.

HVAC units are inspected and serviced monthly to ensure effective operation.

Utility Power and Backup Power Systems
The Internap SEF data center encompasses one floor of the 140 4th Ave North building in Seattle, Washington. Utility power to the building is shared among building residents. The building is supplied with dual 5,000 AMP power feeds from the electric utility. These dual power feeds are split into five "risers" that feed the building floors. For fault tolerance, Internap's redundant UPS systems (with 1296 KW capacity) are fed by all five of these risers. The redundant UPS units condition the power to be supplied to data center equipment, and provide customers with redundant N+1 power feeds to their equipment.

In the event of a utility power outage, the UPS systems automatically switch to backup power from a battery farm which supplies power for up to 20 minutes until the four building-owned 1.5 MW generators power up. Building management maintains 30,000 gallons of on-site fuel which gives the generators capability to power the building for about 8 days at full load. Building management maintains contracts with fuel companies for the delivery of fuel as needed.

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

The building-owned fuel reserves are inspected at least annually to ensure the fuel is viable for the generators.

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 our data centers, ensuring highly technical and customer service focused data center employees. We provide 24/7 manned facilities with a host of security features designed to protect our customer's equipment and network connectivity. We control ingress and egress using electronic keycard software with pin codes, mantraps and biometric scanners. 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:

- 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 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. Customers and employees (including contractors and security guards) must follow a formal access request and approval process 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
- 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.

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

- 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.

An automated security entrance system is utilized to control access in the data center. The systems employ the following key features:

- Monitored/Recorded by CCTV 24/7/365 by Security Control Desk
- 24/7 Intrusion/tampering alarm monitoring by Security Control Desk
- Integrated Card Access Control Systems limit access to authorized individuals

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 approves all requests of Administrator access to the keycard system.

The alarm control system 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

The alarm monitoring and reporting system is equipped and programmed to receive 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 Colocation Space Tracker (CST) application. Update access to the CST CALs is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to CST 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.

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, 2) badge.

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

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

2) badge access - access is controlled via the Ccure system similar to that of data center access. For cages secured via badge access, if access is not disabled for an unauthorized user in Ccure, the access will remain active for both the data center and the customer's cage(s) until it is disabled.

Customer and Employee Access Review
Internap data center security personnel perform a semi-annual audit to validate the appropriateness of all customers' physical access to the data centers. Internap data center security personnel perform a monthly 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
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 (including contractor and 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, an 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, contractors 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 (ie. 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. As such, physical access to the data center is revoked upon termination of Internap employees, contractors and security guards.

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

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 is 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. Cameras are recorded on site via digital video recorders 24/7/365. These visual records are retained for 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

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.

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 our complimentary 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 our data centers.

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

Complimentary 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

- User organizations are responsible for understanding and complying with their contractual obligations.
- User organizations are responsible for ensuring the supervision, management, and control of the use of Internap's services by their personnel.
- User organizations are responsible for designating authorized individuals for access requests to Internap's data center.
- User organizations are responsible for notifying Internap of terminated employees.
- User organizations are responsible for periodically reviewing their Customer Access Lists.
- User organizations are responsible for immediately notifying Internap of any actual or suspected information security breaches, including compromised user accounts.
- User organizations are responsible for notifying Internap of changes made to technical or administrative contact information.
- User organizations are responsible for applying logical access security controls, data encryption controls, and related procedures to their network connected equipment
- User organizations are responsible for the logical protection of their data, including performing backup procedures and classification procedures as necessary.
- User organizations are responsible for protecting their equipment against infection by computer viruses, malicious codes and unauthorized software.
- User organizations are responsible for maintaining their own system components and configurations.
- User organizations are responsible for retaining a terminated employees access badge and either destroying it or returning it to Internap security.
- 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)

Section IV: Description of Test of Controls and Results Thereof

Area 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.
1.2	The entity's system availability and related security policies include, but may not be limited to, the following matters:	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	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	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.		procedures are documented within.	
		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: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	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 other agreements regarding availability	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 performed between April 1, 2011 and September 30, 2011.	No exceptions noted.

This report is intended solely for the use by the management of Internap, its 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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability 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 is performed annually.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.
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.

Section IV: Description of Test of Controls and Results Thereof

Area 2: Communications

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

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.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			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.	
		H - Internal Users (employees) receive 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 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,	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
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.
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 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 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.

Section IV: Description of Test of Controls and Results Thereof

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.

Section IV: Description of Test of Controls and Results Thereof

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 our Customers.	**Inspection** For a sample of data center changes between April 1, 2011 and September 30, 2011, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

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 treats identified.	**Inspection** Inspected documentation to determine whether a third-party data center risk assessment had been performed between April 1, 2011 and September 30, 2011.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment is performed annually.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.
3.2	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	N - A 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 particulate sampling 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 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 at least annually.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

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.	**Inquiry** Inquired of data center management to determine whether the sprinkler system and fire extinguishers are inspected and serviced at least annually. **Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between April 1, 2011 and September 30, 2011.	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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		S - HVAC units are inspected and serviced monthly 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 monthly.	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 April 1, 2011 and September 30, 2011, 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.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

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 quarterly 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 quarterly.	No exceptions noted.
		X - Data center environmental conditions are monitored and reported via the Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alert on Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Alert on Envision for the BACtalk system. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Contractor Requirements.	
		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	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 within between April 1, 2011 and September 30, 2011 to determine whether access was approved by Data Center Management.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
	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)	CC - Physical access to the data center is revoked upon termination of Internap employees, contractors and security guards.	**Inspection** Inspected the active keycard listing for a sample of terminated employees to determine whether physical access to the data center is revoked upon termination of Internap employees, contractors and security guards.	No exceptions noted.
		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 a sample of 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.
		EE - Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.	**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 determine whether customer equipment is segregated via locked cages or locked cabinets such that customers can only access their	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			own equipment.	
		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 audit to determine whether Internap collocation security personnel perform a semi-annual audit 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.	Exception noted: One individual, whose access was requested to be deleted, retained add/modify/delete access to the Ccure badge access system. Additional Procedures: Through corroborative inquiry and inspection of job titles, determined that the user's access in question was appropriate.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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, security guards, and customers who were granted physical access to the data center between April 1, 2011 and September 30, 2011 to determine whether only authorized Internap employees, contractors, security guards, and customers are granted physical access to the data center.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		AA - User update access to CST 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 customer contact lists to determine whether access is limited to authorized personnel only.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
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, security guards, and customers who were granted physical access to the data center between April 1, 2011 and September 30, 2011 to determine whether only authorized Internap employees and customers are granted physical access to the data center.	No exceptions noted.
		CC - Physical access to the data center is revoked upon termination of Internap employees, contractors and security guards.	**Inspection** Inspected the active keycard listing for a sample of terminated employees to determine whether 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** For a sample of customer employees who require data center access revocation, inspected Ccure keycard access listings to determine whether unauthorized customer employee access had been removed.	Exception noted. For one of a sample of two customer employee access revocation requests, the unauthorized customer employee's access was not removed from the Ccure keycard access system. Additional Procedures Performed: Tested the entire population of five customer employee access revocation requests with no

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
				additional exceptions noted. Inspected the Ccure log of badge access for the exposure period and determined the customers' employee in question had not accessed the data center.
		EE - Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.	**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 determine whether customer equipment is segregated via locked cages or locked cabinets such that customers can only access their own equipment.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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 via a combination of key card and biometric technology to gain physical access to the data center. **Observation** Observed successful and unsuccessful attempts to gain entry to the data center to determine whether employees and customers must be validated via a combination of key card and biometric technology.	No exceptions noted.
		GG - A manned security post controls entry into Internap data centers.	**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 to determine whether 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.	**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	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			monitored by Internap personnel.	
		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 monthly audit to validate the appropriateness of all employees', contractors', and security guards' physical access to the data centers.	**Inspection** Inspected a sample of monthly audits of employees, contractors, and security guards with data center access to determine whether the reviews were performed and access changes requested were implemented.	Exception noted: The access listings reviewed do not include users categorized as 'sales', contractors', or 'security' in the Ccure badge system that have physical access to the data center.
		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 a sample of 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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
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 new hire training and are made aware of the customer facing documents and other internal policies covering data center security and availability.	**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.
		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;	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Instrumentation Measuring; Equipment Tests; Security Procedures; Safety Procedures; Network Area and Workroom Procedures; Colocation Procedures and SLA; and Contractor Requirements.	
		X - Data center environmental conditions are monitored and reported via the Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alert on Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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 Alert on Envision for the BACtalk system.	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	
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 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 at least annually.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability 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.	**Inquiry** Inquired of data center management to determine whether the sprinkler system and fire extinguishers are inspected and serviced at least annually. **Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between April 1, 2011 and September 30, 2011.	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 April 1, 2011 and September 30, 2011, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.
		S - HVAC units are inspected and serviced monthly 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 monthly.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability 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 third-party vendor preventative maintenance and inspection report to determine whether UPS systems are inspected and serviced at least annually.	No exceptions noted.
		W - Generators are inspected and serviced at least quarterly 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 quarterly.	No exceptions noted.
		X - Data center environmental conditions are monitored and reported via the Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alert on Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			Center (NOC) to determine whether power, HVAC, temperature, and fire detection/suppression conditions are monitored and reported via the Alerton Envision for the BACtalk system. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 performed between April 1, 2011 and September 30, 2011.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment is performed annually.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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.
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 April 1, 2011 and September 30, 2011, 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 April 1, 2011 and September 30, 2011 to determine whether an employment pre-screening process is in place and includes background, credit and DMV checks where applicable based	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			on job requirements.	
		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.	**Inquiry** Inquired of management to determine whether an annual performance review has been performed for each employee.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.
		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.
		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.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
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 April 1, 2011 and September 30, 2011, inspected Critical Environment Work Authorization (CEWA) forms to determine whether the work had been properly reviewed and approved.	No exceptions noted.
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 April 1, 2011 and September 30, 2011, inspected Critical Environment Work Authorization (CEWA)	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			forms to determine whether the work had been properly reviewed and approved.	

Section IV: Description of Test of Controls and Results Thereof

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 Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alerton Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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 Alerton Envision for the BACtalk system. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk console which	No exceptions noted.

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
			reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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.

Section IV: Description of Test of Controls and Results Thereof

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 Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alerton Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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 Alerton Envision for the BACtalk system. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		N - A 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 particulate sampling 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 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 at least annually.	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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability 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.	**Inquiry** Inquired of data center management to determine whether the sprinkler system and fire extinguishers are inspected and serviced at least annually. **Inspection** Inspected evidence to determine whether the fire extinguishers and fire suppression system were serviced between April 1, 2011 and September 30, 2011.	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 performed between April 1, 2011 and September 30, 2011.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment is performed annually.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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.
		S - HVAC units are inspected and serviced monthly 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 monthly.	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.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability 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 third-party vendor preventative maintenance and inspection report to determine whether UPS systems are inspected and serviced at least annually.	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.
		W - Generators are inspected and serviced quarterly 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 quarterly.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

Ref. #	Availability Criteria	Control Activities	Tests of Operating Effectiveness	Results of Tests
		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.

Section IV: Description of Test of Controls and Results Thereof

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 Alerton Envision for BACtalk system. Data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk 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 Alerton Envision for the BACtalk system and whether data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor BACtalk 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 Alerton Envision for the BACtalk system. Observed data center technicians and Internap's centralized Network Operations Center (NOC) personnel monitor the BACtalk console which reports the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	No exceptions noted.

Section IV: Description of Test of Controls and Results Thereof

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 performed between April 1, 2011 and September 30, 2011.	No exceptions noted.
		M - The Company performs an enterprise wide risk assessment annually.	**Inquiry** Inquired of management to determine whether an enterprise risk assessment is performed annually.	Not applicable. This control has not operated between April 1, 2011 and September 30, 2011 due to its planned frequency.