INDEPENDENT SERVICE AUDITOR'S REPORT

INTERNAP HOLDING LLC:

ACS – Atlanta, GA
BSN003 – Boston, MA
DAL006 – Dallas, TX
LAX014 – Redondo Beach, CA
NYJ004 – Secaucus, NJ
PHX – Phoenix, AZ
SEF – Seattle, WA
SEF003 – Tukwila, WA
SJE011 – Santa Clara, CA

Flagship Data Center Services

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

For the Period
October 1, 2019 to September 30, 2020

UHY LLP
Certified Public Accountants

Internap Holding LLC

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

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR’S REPORT

To the Board of Directors of Internap Holding LLC:

Scope

We have examined Internap Holding LLC’s (“INAP”) accompanying description of its colocation data center services found in Section III titled “Description of the Internap Holding LLC System – Internap United States Data Center Services” throughout the period October 1, 2019 to September 30, 2020 (“description”) based on the criteria for a description of a service organization’s system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (“AICPA *Description Criteria”*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that INAP’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (“applicable trust services criteria”) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (“AICPA *Trust Services Criteria”*).

The information included in Section V, “Other Information Provided by Internap Holding LLC,” is presented by INAP management to provide additional information and is not a part of INAP's description of its system made available to user entities during the period October 1, 2019 to September 30, 2020. Information about INAP management’s responses to testing exceptions has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at INAP, to achieve INAP’s service commitments and system requirements based on the applicable trust services criteria. The description presents INAP's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of INAP’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

INAP is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that INAP’s service commitments and system requirements were achieved. In Section II, INAP has provided an accompanying assertion titled Management’s Assertion (“assertion”) about the description and the suitability of design and operating effectiveness of controls stated therein. INAP is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects;

a. the description presents INAP’s data center services system that was designed and implemented throughout the period October 1, 2019 to September 30, 2020 in accordance with the description criteria,

b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that INAP’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary user entity controls assumed in the design of INAP 's controls throughout that period,

c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that INAP’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of INAP’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of INAP, user entities of INAP's data center services system during some or all of the period October 1, 2019 to September 30, 2020, business partners of INAP subject to risks arising from interactions with the data center services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, and other parties
- internal control and its limitations
- user entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization's services
- the applicable trust services criteria
- the risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks
- complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements

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

UHY LLP

Atlanta, GA
February 13, 2021

II. MANAGEMENT’S ASSERTION

Assertion of the Management of Internap Holding LLC:

We have prepared the accompanying description of Internap Holding LLC’s (“INAP”) data center services system titled “Description of the Internap Holding LLC System – Internap United States Data Center Services” throughout the period October 1, 2019 to September 30, 2020 (description) based on the criteria for a description of a service organization’s system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the data center services system that may be useful when assessing the risks arising from interactions with INAP’s system, particularly information about system controls that INAP has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at INAP, to achieve INAP’s service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents INAP’s data center services system that was designed and implemented throughout the period October 1, 2019 to September 30, 2020 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that INAP’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of INAP’s controls throughout that period.
3) The controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that INAP’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of INAP’s controls operated effectively throughout that period.

Signature:
Title: Executive Vice President & General Counsel

III. DESCRIPTION OF THE INTERNAP HOLDING LLC SYSTEM – INTERNAP UNITED STATES DATA CENTER SERVICES

Company Background and Service Offerings

Internap Holding LLC ("INAP" or "Company") is the high-performance Internet infrastructure provider that powers the applications shaping the way we live, work, and play. INAP's hybrid infrastructure delivers performance without compromise – blending virtual and bare-metal cloud, hosting, and colocation services across a global network of data centers, optimized from the application to the end user and backed by rock-solid customer support and a 100% uptime guarantee. Since 1996, companies have relied on INAP to make their applications faster and more scalable.

INAP operates in two business segments: Data Center and Network Services, which includes Colocation and IP services, and Hosting Services. The scope of this report focuses on data center services, which primarily include physical space for collocating customers' network and other equipment plus associated services such as redundant power, environmental controls, and security.

INAP uses a combination of facilities that are operated by INAP and by third parties, referred to as INAP datacenters and non-core sites, respectively. INAP charges monthly fees for data center services based on the amount of square footage and power that a customer uses. This report is related to the following INAP data centers:

- Atlanta (ACS), 250 Williams Street, Suite E100, Atlanta, GA 30303
- Boston (BSN003), 50 Inner Belt Road, Somerville, MA 02143
- Dallas (DAL006), 1221 Coit Road, Plano, TX 75075
- Los Angeles (LAX014), 3690 Redondo Beach Ave, Redondo Beach, CA 90278
- Secaucus (NYJ004), 1 Enterprise Ave North, Secaucus, NJ 07094
- Phoenix (PHX), 2500 West Frye Rd. Chandler, AZ 85248
- Seattle (SEF), 140 4th Ave North, Suite 200, Seattle, WA 98019
- Tukwila (SEF003), 3355 S 120th Place, Tukwila, WA 98168
- Santa Clara (SJE011), 2151 Mission College Blvd, Santa Clara, CA 95054

Principal Service Commitments and System Requirements

INAP's service commitments to customers for colocation services include providing physically secure and conditioned space for customer equipment.

INAP must install and maintain security systems to control access to data centers and shared common space and provide customers with key cards or other such technology to access the facilities. Customers may access secured data centers 24 hours a day, 7 days a week, 365 days a year ("24/7/365") unless otherwise specified. Access to customer cages or cabinets must be limited to individuals authorized by the customer, except for instances where INAP personnel must access for maintenance or emergency purposes. Otherwise, consent must be obtained from the customer prior to INAP accessing their space. INAP must ensure that there is no unauthorized access.

INAP must condition the data center to ensure that the power supply to customer equipment is uninterrupted, using a combination of UPS and backup generator systems. Uninterrupted cooling must be provided to customer space.

For customers which have purchased and installed a redundant power solution, INAP must use commercially reasonable efforts to ensure that power will be available to the customer's cage, cabinet, rack, or suite 100% of the time except as part of scheduled maintenance or by request from the customer. In instances where customers do not have a redundant power solution, INAP must use commercially reasonable efforts to ensure that customers will not experience an event lasting more than 15 minutes except as part of scheduled maintenance or by request from the customer.

INAP must use commercially reasonable efforts to ensure that the temperature in INAP's colocation areas will not fall below 65 degrees Fahrenheit or rise above 80 degrees Fahrenheit. INAP must use commercially reasonable efforts to ensure that humidity in INAP's colocation areas will not fall below 20% or rise above 80% relative humidity.

In order to ensure these commitments are met and to ensure the safety of its data centers, INAP must regularly inspect and service power and cooling equipment.

The Aspects of the System and a Description of its Boundaries

INAP is primarily responsible for the following types of activities related to data center services at its datacenters:

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

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

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

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

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

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

Risk Assessment

INAP uses various methods to manage risks that could impact the Company's ability to deliver service to customers. Management assesses risks that inherently arise from the expansion of the business, whether organically or inorganically. This may include managing risks that are rooted in changes in personnel, technology, or the Company's operating environment. Additionally, management engages security experts to periodically assess risks to the achievement of security and availability objectives. Management revisits these assessments annually to ensure these risks are appropriately mitigated. Lastly, management performs an annual companywide risk assessment, which includes INAP datacenters.

Information and Communication Systems

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

Monitoring

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

There have not been any known instances of security breaches affecting customer equipment or data during the period under review. There have not been any instances of extensive service outages during the period under review.

Control Environment and Policy and Procedural Components

INAP IT policies and procedures are documented and are readily available to employees. The responsibility and accountability for changes and updates to these policies are assigned to appropriate IT management personnel. The information in these policies is reviewed on an annual basis by IT management.

INAP 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. The information in these policies is reviewed on an annual basis by appropriate data center employees.

Each INAP data center has a specific Data Center Operations Manual kept in a binder and physically available for 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) uses 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. INAP personnel use a ticketing system to track incidents and customer requests. Incidents are escalated as necessary and tracked until resolution.

Each customer in INAP data centers is given Customer Service documentation. These documents include 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 Service documents is reviewed on an annual basis by business unit management to ensure the information is up-to-date and accurate. Additionally, INAP customers connect to INAP via the INAP website and online customer portal. INAP's website hosts a detailed description of the data center services and the portal houses customer specific information and enables customers to contact INAP directly through the system. This customer portal, along with ad hoc communication methods are used to ensure transparent communication with customers.

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

Infrastructure, Environmental, and System Monitoring Components

INAP's data center operations consist of a strong physical infrastructure, including secure facilities featuring N+1 redundancy for both power and cooling, along with fire protection and system monitoring. The existing facility and environmental standards at the data centers are designed to ensure that uptime is maximized by providing redundancy to key facility and environmental systems.

Monitoring Environmental Conditions and Critical Work Authorizations

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

INAP has in place a Change Management process to ensure all scheduled maintenance and other data center implementations/modifications are documented and authorized to assure minimal impact to the customers. Threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact) in the company's Business Continuity Plan.

Smoke / Fire Detection

The smoke and fire detection system in the 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 defense against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room, and the BMS generates alerts to INAP employees.

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

Fire Suppression

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

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

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

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

Heating, Ventilation, and Air Conditioning (HVAC)

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

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

Utility Power and Backup Power Systems

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

Each of INAP's data centers maintain contracts with fuel companies for the delivery of fuel as needed.

The UPS systems and generators are inspected and serviced at least annually to ensure effective operation. The operating effectiveness of backup power systems are confirmed at least annually, through load bank testing and / or other methods.

Personnel, Security, and Software System Components

INAP's commitment to competence includes management's determination of the levels of competence and expertise required for each position at the data center, ensuring highly technical and customer service focused data center employees. INAP provides 24/7/365 manned facilities with a host of security features designed to protect the customer's equipment and network connectivity. INAP controls ingress and egress using electronic keycard and / or biometric software. All cages and cabinets are securely locked and Closed-Circuit Television (CCTV) cameras monitor and record activity within each facility.

Organizational Structure and Assignment of Authority and Responsibility

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

Human Resource Policies and Practices

INAP'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. The Company has a written Code of Conduct that is communicated to and certified by all employees annually. The Code details the Company's expectations regarding behavior, ethics, and business practices that every employee must abide by.

Detailed job descriptions and organizational charts convey the requirements for each position. INAP also facilitates employee development through annual evaluations, onsite training, and the allocation of funds for other relevant training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with INAP. 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, INAP 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 INAP's data center security resources. Such outsourcing ensures consistency of training, performance, metrics, and supervision. Responsibilities of security personnel include, but are not limited to the following.

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

Security Control

All INAP data centers have Security and/or INAP Data Center personnel to control access, monitor security alarms, monitor CCTV camera surveillance, and support security-related operational activities 24/7/365. Security personnel and/or INAP on-duty engineers are onsite 24/7/365. The Security Control Desk performs the following.

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

Surveillance and Monitoring

INAP data centers employ a CCTV system 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.

INAP personnel monitor the signals from the CCTV system. The desk is connected by secure cables to the cameras throughout the facility to permit both interior and exterior surveillance.

Cameras are recorded onsite via digital video recorders 24/7/365. These visual records are retained for at least 90 days to provide details of activity at INAP data centers. INAP provides dedicated 24/7/365 continuous power supply (CPS) and standby emergency power via generator to support security systems.

Access Control

INAP employs a computerized Access Control System (ACS) to control physical access to the data centers. The ACS utilizes proximity card readers with pin codes or biometrics to control access into the data center floor, perimeter doors, shipping & receiving areas, storerooms, and other critical areas. Customers and employees (including contractors and security guards) must follow formal access request and approval processes before physical access to the 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.
- INAP access badges and / or biometrics are required to gain entry to critical areas.
- Customers, Vendors, Contractors, Visitors and non-data center employees must sign in at the security desk prior to entry into the data center. INAP personnel verifies log accuracy and reconciles log with ACS.
- Customers, Vendors, Contractors, and other Visitors must be sponsored by an INAP-approved host to gain access if not on the Customer-Approved List.
- All Customers, Vendors, Contractors, and Visitors on the Customer-Approved List must check in with the Security Desk upon arrival with photo identification if they require the physical key to access cages. Those customers with badge cage access will have automatic access to their cages.
- Visitors and others not on the Customer-Approved List are escorted while in the data center and other critical areas.
- Guest access for approved Contractors is generally limited to particular areas where work is being performed. Long term contractors are granted more general access via personal badges.
- Employees with access to the data center are limited to those with a specific business need or job function.

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

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

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

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

Visitor / Sales Tour Access

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

Customer Access

Each customer is permitted to designate individuals with access to INAP 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 (CALs) within the Facility Management application. Update access to the CAL is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to the CALs and will only allow individuals listed on a Company's CAL access to the data center. The customer is responsible for requesting additions, modifications, or deletions to access. Upon notification of a customer employee termination or revocation of customer agreement, physical access to the data center is revoked. Customers are responsible for retaining a terminated employee's access badge and either destroying it or returning it to INAP security.

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

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

1. Physical key - Keys are maintained by INAP security personnel or INAP onsite engineer. After the security personnel or INAP onsite engineer determine appropriate authority per the CAL, they escort the customer to the cage and unlock it for them; or
2. Badge reader access - access is controlled via the ACS, similar to that of data center access.

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

1. Physical key - Keys are maintained by INAP security personnel and INAP onsite engineer. After the security personnel or INAP onsite engineer determine appropriate authority per the CAL, they escort the customer to the cabinet and unlock it for them; or
2. Combination lock - access is controlled via the use of a customer specific combination code.

Customers are responsible for ensuring their cage and cabinet(s) are properly locked before leaving the facility.

Employee and Security Guard Access to Data Center

Access to the data center is restricted to only those INAP 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 INAP employees and security guards.

Contractor and Vendor Access to Data Center

Access to the data center is restricted to Contractors and Vendors with a legitimate business purpose. Access is granted with a daily temporary badge and logged with Security unless the Contractor or Vendor will be onsite for an extended period of time or multiple times over an extended period (e.g., 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 the facilities. If a temporary badge is not returned at the end of the day, it is disabled in the system by Security. Physical access to the data center is revoked upon completion of the contractors' and / or vendors' duties.

General Visitor Rules

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

Customer and Employee Access Review

INAP personnel perform audits to validate the appropriateness of access permissions in the Access Control System (ACS). The following audits are performed.

1. Customer access permissions in the ACS are validated against the Facilities Access list at least quarterly and discrepancies are investigated and remediated appropriately.
2. Employee, Contractor, and Security Guard access in the ACS are reviewed for appropriateness at least quarterly.
3. Employees with access to add, modify, and delete users in the ACS are reviewed for appropriateness at least annually.

Logical and Network Protections for the Access Control System and Facility Management Application

Access to the network and applications is ID and password protected. Roles based access to applications and operating systems ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.

Password length and complexity requirements are established for the INAP internal network. Password settings for the keycard system are the same as for the internal network since the system uses single sign on.

Anti-virus software for network workstations and keycard system servers is installed and operating effectively. The Company has firewalls in place to limit access over the internet to the central keycard system application and database. Connections via VPN tunnel between company locations are protected using encryption. Connections to applications via the internet are protected using encryption.

Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the appropriate business unit representative for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.

Data Used and Supported by the System

Client Data

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

Data Managed by INAP

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

Physical Access Control System Lists and Key Badges – INAP maintains a listing of all individuals with physical access to the data center. This is managed using the Access Control System. Customers may request a report listing all individuals who have physical access to their cage or cabinet. Customers are responsible for periodically reviewing their access lists and for notifying INAP of terminated employees.

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

Significant Changes to the System during the Review Period

There were no significant changes to the data center services system during the period.

Trust Services Criteria Determined to be Not Applicable

INAP's operations, as described above, address all of the applicable Trust Services criteria related to the security and availability categories, with the exception of the following criterion, which is not applicable to INAP's colocation data center services:

- Common Control 6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

  INAP's Response:

  INAP is not responsible for disposition of its customer's assets as part of providing colocation services.

Complementary User Entity Control Considerations

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

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

- User entities are responsible for understanding and complying with their contractual obligations. (all criteria)
- User entities are responsible for ensuring the supervision, management, and control of the use of INAP's services by their personnel. (all criteria)
- User entities are responsible for establishing a data classification process and classifying their data to determine criticality and ensure necessary controls and protections are in place. (criteria CC6.1)
- User entities are responsible for designating authorized individuals for access requests to INAP's data center. (criteria CC6.4)
- User entities are responsible for notifying INAP of additions, modifications, and deletions of authorized physical access to their equipment. (criteria CC6.2, CC6.3, and CC6.4)
- User entities are responsible for retaining a terminated employee's access badge and either destroying it or returning it to INAP Security. (criteria CC6.4)
- User entities are responsible for changing their cabinet combination lock password after individuals with knowledge of the current combination are terminated. (criteria CC6.4)
- User entities are responsible for periodically reviewing their Customer Access Lists. (criteria CC6.4)
- User entities are responsible for immediately notifying INAP of any actual or suspected information security breaches, including compromised user accounts. (criteria CC7.2, CC7.3, CC7.4)
- User entities are responsible for notifying INAP of changes made to technical or administrative contact information. (criteria CC6.4)
- User entities are responsible for ensuring their employees properly lock their cage or cabinet before leaving INAP facilities. (criteria CC6.4)
- User entities are responsible for applying logical access security controls, data encryption controls, and related procedures to their network connected equipment. (criteria CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.7, and CC6.8)
- User entities are responsible for protecting their equipment against infection by computer viruses, malicious codes, and unauthorized software. (criteria CC6.7, CC6.8, CC7.1, and CC7.2)

- User entities are responsible for protecting and maintaining the network security of system resources (e.g., secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services). (criteria CC6.1, CC6.6, CC7.1, CC7.2, CC7.3, CC7.4, and CC7.5)
- User entities are responsible for maintaining their own system components and configurations. (criteria CC6.5, CC7.1 and CC8.1) *NOTE: As a result of this complementary user entity control (CUEC), CC6.5 is deemed Not Applicable for INAP.*
- User entities are responsible for periodically identifying and assessing risk related to services outsourced to third parties and for developing risk mitigation activities as needed. (criteria CC9.1 and CC9.2)
- User entities are responsible for maintaining, monitoring, and evaluating the capacity and usage of their systems' bandwidth and processing requirements. (criteria A1.1)
- User entities are responsible for the logical protection of their data, including performing backup procedures and periodically testing system and data recovery plans as necessary. (criteria A1.2, A1.3)

IV. INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITORS

Scope of the Testing

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

The type of tests that may have been performed on the effectiveness of controls detailed in the following section include:

TEST	DESCRIPTION
Inquiry	Made inquiries of the appropriate service organization staff. Inquiries seeking relevant information or representation from service organization personnel were performed to obtain: • Knowledge and additional information regarding the policy and procedure. • Corroborating evidence of the policy or procedure.
Observation	Observed application of specific controls.
Inspection	Inspected documents and reports that indicate performance of the control structure policy or procedures. This includes among other things: • Testing of source documents to ensure transactions processed were consistent with transaction requests and that such transactions were in compliance with control structure policies. • Reviewing of source documentation and authorization to verify propriety and timeliness of transactions processed.
Re-performance	Independently performed procedures or controls originally performed by the service organization as part of their internal control.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The Code of Conduct provides standards on conduct, integrity, and ethical values. The Code of Conduct is provided to employees during onboarding and is available on INAP's intranet. Employees are required to periodically acknowledge that they have read, understood, and complied with the code.	Inspected the Code of Conduct to verify that the document outlined standards on conduct, integrity and ethical values. Inspected a screen shot of the Code of Conduct published to the Company's internet site to verify that the Code of Conduct was available to employees. Inspected the Code of Conduct acknowledgements for a sample of new and existing employees to verify that each employee acknowledged they had read, understood, and agreed to comply with the Code of Conduct during the on-boarding process and annually thereafter.	No exceptions noted.
		An Ethics Hotline (Whistleblower Line) is available for employees and external parties to anonymously report fraud, violations of company policies, unethical behavior, and other issues. The Ethics Committee reviews and investigates reported ethics incidents and takes appropriate action in response to violations of the Code of Conduct. According to the Code of Conduct, anyone making such a report is protected from retaliation.	Inspected the Ethics Hotline reporting instructions published to INAP's intranet and public facing website to verify that INAP made its Ethics Hotline available officers, employees, third parties, and external parties and included information on how to report fraud, violations, unethical behavior, and other concerns. Inspected the ethics incident reports Code of Conduct violations to verify that each incident was reported to the Ethics Committee, investigated, and took appropriate actions. Inspected the Company Policy and Code of Conduct to verify that a policy was in place to protect persons submitting ethics reports from retaliation.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	INAP has an independent Board of Directors with clear duties, responsibilities and purpose articulated in the Corporate Governance Guidelines. The Board of Directors provides management oversight responsibilities.	Inspected the Corporate Governance Guidelines and Audit and Finance Committee Charter to verify that the guidelines and charter - • articulated the Board of Directors' (BOD) duties, responsibilities and purpose • provided detailed guidance on board composition, nominations, compensation review, responsibilities, and committees; orientation and education; meetings/agendas; evaluations and planning; self-assessment; and interactions with third parties and employees	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	INAP has an independent Board of Directors with clear duties, responsibilities and purpose articulated in the Corporate Governance Guidelines. The Board of Directors provides management oversight responsibilities.	Inspected the Corporate Governance Guidelines and Audit and Finance Committee Charter to verify that the guidelines and charter - • articulated the Board of Directors' (BOD) duties, responsibilities and purpose • provided detailed guidance on board composition, nominations, compensation review, responsibilities, and committees; orientation and education; meetings/agendas; evaluations and planning; self-assessment; and interactions with third parties and employees	No exceptions noted.
		INAP has a formal corporate organizational structure appropriate for the size of the organization. Organizational charts are in place documenting reporting lines and responsibilities.	Observed the organizational chart to verify that INAP had a formal organizational structure showing the reporting structure and responsibilities.	No exceptions noted.
		Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.	Inspected the role descriptions for a sample of positions to verify that the minimum requirements, experience requirements, roles and responsibilities were defined for each position.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Human Resources policies and procedures are in place providing a framework for hiring, training, promoting, and compensating employees across the organization. An employment prescreening process is performed for new hires, which includes background, credit, and DMV checks (based on job requirements).	Observe the prescreening documentation for a sample of new hires to verify that Human Resources obtained background, credit, and/or DMV checks for each new hire as part of the employment prescreening process.	No exceptions noted.
		INAP has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to verify that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected the current year's employee performance review tracking spreadsheet to verify that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
		Internal Audit maintains an active listing of control owner assignments for each SOC 2 and PCI control activity. Control design and coverage is assessed at least annually by Internal Audit with the control owners.	Inspected the risk and controls matrices and control design review meeting invitations to verify that Internal Audit maintained an active listing of SOC 2 and PCI control owner assignments and that they were reviewed with the control owners at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.	Inspected the role descriptions for a sample of positions to verify that the minimum requirements, experience requirements, roles and responsibilities for internal control were defined for each position.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 1	**Common Criteria Related to Control Environment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to verify that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected the current year's employee performance review tracking spreadsheet to verify that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
		Internal Audit maintains an active listing of control owner assignments for each SOC 2 and PCI control activity. Control design and coverage is assessed at least annually by Internal Audit with the control owners.	Inspected the risk and controls matrices and control design review meeting invitations to verify that Internal Audit maintained an active listing of SOC 2 and PCI control owner assignments and that they were reviewed with the control owners at least annually.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
		IT staff monitor critical/relevant systems for errors or exceeded thresholds. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined thresholds.	Inspected the alerting configuration and examples of alerts to verify that systems were configured to notify IT staff when conditions exceed defined thresholds. Inspected the error log to verify that errors were logged when conditions exceeded defined thresholds.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		INAP data center power and environmental conditions are monitored and reported via automated monitoring systems. INAP personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Observed the BMS monitoring and reporting system and alerts received by INAP personnel to verify that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
		Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to verify that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Role descriptions exist for all key positions, which define minimum requirements, experience requirements, and roles and responsibilities.	Inspected the role descriptions for a sample of positions to verify that the minimum requirements, experience requirements, roles and responsibilities for internal control were defined for each position.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to verify that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected the current year's employee performance review tracking spreadsheet to verify that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
		Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	Common Criteria Related to Communication and Information			
Criteria		Service Organization Control Activity	Test Performed by the Service Auditor	Test Results
		The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management annually and available to employees on SharePoint.	Inspected INAP policies and procedures to verify that * INAP maintained IT related policies and procedures, including Information Security, Change Management, and other operational and conduct policies * the policies and procedures included objectives and responsibilities for internal control * the policies and procedures were reviewed and approved by management annually. Inspected a screen shot of the policies and procedures published to the Company's SharePoint site to verify that the IT policies and procedures were available to employees.	No exceptions noted.
		Each INAP Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management on an annual basis.	Inspected the Data Center Operations Manual for each INAP data center to verify that each INAP Company controlled data centers had a Data Center Operations Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management on an annual basis	No exceptions noted.
		INAP's Network Operations Center (NOC) procedures are in place which are available to NOC personnel to provide guidance on responding to requests and issues. The NOC procedures are reviewed and approved by management on an annual basis.	Inspected INAP's NOC procedures to verify that the procedures were available to NOC personnel, included guidance for responding to requests and issues, and reviewed and approved by management on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 2	**Common Criteria Related to Communication and Information**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The process for customers to inform INAP of system availability issues, possible security breaches, and other incidents is provided in the Customer Service documents and/or online customer webpage. The Customer Service documents are reviewed and approved by management on an annual basis.	Inspected the Customer Service documents and customer webpage to determine that the process for customers to inform INAP of system availability issues, security breaches, and other incidents was provided in the Customer Service documents and/or customer webpage, and the Customer Service documents were reviewed and approved by management on an annual basis.	No exceptions noted.
		The Company has in place a Change Management process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	Inspected the data center infrastructure change tickets/forms for a sample of infrastructure changes to verify that the INAP had a Change Management process in place to ensure all scheduled maintenance and other data center implementations / modifications were properly documented and authorized to assure minimal impact to customers. Inspected the customer notifications for a sample of scheduled maintenance or other changes that could affect customer availability to verify that customers were notified in advance.	No exceptions noted.
		The scope of services agreed to with new vendor service providers which could impact the security and availability of INAP data centers, as well as any compliance or security requirements and SLAs that the vendor must adhere to, are documented in contractual agreements with the vendor.	Inspected the contractual agreements for a sample of vendors to verify that the scope and any service, compliance or security requirements were documented in the vendor contractual agreements.	No exceptions noted.

<table>
<tr><th colspan="5">COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES</th></tr>
<tr><th>CC 3</th><th colspan="4">Common Criteria Related to Risk Assessment</th></tr>
<tr><th colspan="2">Criteria</th><th>Service Organization Control Activity</th><th>Test Performed by the Service Auditor</th><th>Test Results</th></tr>
<tr><td rowspan="2">CC3.1</td><td rowspan="2">The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</td><td>INAP has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.</td><td>Inspected the performance evaluation template to verify that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process.
Inspected the current year's employee performance review tracking spreadsheet to verify that Human Resources tracked completion and results of the annual assessment.</td><td>No exceptions noted.</td></tr>
<tr><td>The Company performs an annual risk assessment which includes internal and external risks, such as economic conditions, business and industry risks, competitor risks, IT infrastructure risks, cybersecurity risks, customer retention risks, capital investment risks, regulations, fraud, changes in the business model, changes in leadership, and other risk areas. The results of the risk assessment are communicated to management.</td><td>Inspected the most recently completed risk assessment to verify that a risk assessment was conducted annually and identified and assessed risks to the Company's objectives.</td><td>No exceptions noted.</td></tr>
</table>

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The Company performs an annual risk assessment which includes internal and external risks, such as economic conditions, business and industry risks, competitor risks, IT infrastructure risks, cybersecurity risks, customer retention risks, capital investment risks, regulations, fraud, changes in the business model, changes in leadership, and other risk areas. The results of the risk assessment are communicated to management.	Inspected the most recently completed risk assessment to verify that a risk assessment was conducted annually, identified risks to the achievement of its entity wide objectives and analyzed risk as a basis for how the risk should be managed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
		Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of INAP data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how INAP data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to INAP systems, and other risk factors.	Inspected the vendor risks assessments for a sample of new vendors to verify that a vendor risk assessment was performed and considered security and availability related risks such as vendor access rights; data exchanges, transmissions, processing and storage; and access to INAP systems.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		The Company performs an annual Cybersecurity Risk Assessment to identify risks and assess the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk assessment to verify that INAP identified risks and assessed risk mitigation controls on an annual basis. Inspected the cybersecurity risk register to verify that risk items and remediation plans were tracked until resolved.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The Company performs an annual risk assessment which includes internal and external risks, such as economic conditions, business and industry risks, competitor risks, IT infrastructure risks, cybersecurity risks, customer retention risks, capital investment risks, regulations, fraud, changes in the business model, changes in leadership, and other risk areas. The results of the risk assessment are communicated to management.	Inspected the most recently completed risk assessment to verify that a risk assessment was conducted annually and considered the potential for fraud in assessing risks to the achievement of the Company's objectives.	No exceptions noted.
		An Ethics Hotline (Whistleblower Line) is available for employees and external parties to anonymously report fraud, violations of company policies, unethical behavior, and other issues. The Ethics Committee reviews and investigates reported ethics incidents and takes appropriate action in response to violations of the Code of Conduct. According to the Code of Conduct, anyone making such a report is protected from retaliation.	Inspected the Ethics Hotline reporting instructions published to INAP's intranet and public facing website to verify that INAP made its Ethics Hotline available officers, employees, third parties, and external parties and included information on how to report fraud, violations, unethical behavior, and other concerns. Inspected the ethics incident reports Code of Conduct violations to verify that each incident was reported to the Ethics Committee, investigated, and took appropriate actions. Inspected the Company Policy and Code of Conduct to verify that a policy was in place to protect persons submitting ethics reports from retaliation.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The Company performs an annual risk assessment which includes internal and external risks, such as economic conditions, business and industry risks, competitor risks, IT infrastructure risks, cybersecurity risks, customer retention risks, capital investment risks, regulations, fraud, changes in the business model, changes in leadership, and other risk areas. The results of the risk assessment are communicated to management.	Inspected the most recently completed risk assessment to verify that the Company identified and assessed changes the could significantly impact the system of internal control.	No exceptions noted.
		Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 3	**Common Criteria Related to Risk Assessment**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Vulnerability scans are performed at least quarterly for the internal corporate networks and identified vulnerabilities are assessed. Vulnerabilities are communicated to the owner of the IT asset and tracked by IT until remediation.	Inspected the vulnerability scan results for a sample of quarters to verify that vulnerability scans of the internal corporate network were performed at least quarterly and identified vulnerabilities were assessed. Inspected the remediation tickets for a sample of vulnerabilities identified during the quarterly vulnerability scans to verify that vulnerabilities were communicated to the owner of the IT asset and tracked by IT until remediation.	No exceptions noted.
		Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of INAP data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how INAP data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to INAP systems, and other risk factors.	Inspected the vendor risks assessments for a sample of new vendors to verify that a vendor risk assessment was performed and considered security and availability related risks such as vendor access rights; data exchanges, transmissions, processing and storage; and access to INAP systems.	No exceptions noted.
		The Company performs an annual Cybersecurity Risk Assessment to identify risks and assess the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk assessment to verify that INAP identified risks and assessed risk mitigation controls on an annual basis. Inspected the cybersecurity risk register to verify that risk items and remediation plans were tracked until resolved.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
		Application access, as well as database, and operating system privileged access, is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed privileged user access review to verify that management reviewed users' privileged access to application, database and operating system on an annual basis to ensure access is commensurate with job responsibilities.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		Vulnerability scans are performed at least quarterly for the internal corporate networks and identified vulnerabilities are assessed. Vulnerabilities are communicated to the owner of the IT asset and tracked by IT until remediation.	Inspected the vulnerability scan results for a sample of quarters to verify that vulnerability scans of the internal corporate network were performed at least quarterly and identified vulnerabilities were assessed. Inspected the remediation tickets for a sample of vulnerabilities identified during the quarterly vulnerability scans to verify that vulnerabilities were communicated to the owner of the IT asset and tracked by IT until remediation.	No exceptions noted.
		User access to add, modify, and delete users in INAP's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspect the most recently performed keycard system reviews to verify that individuals with access to add, modify, and delete users in the keycard system were reviewed for appropriateness based on their job responsibilities on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP data centers are monitored 24/7/365 by security guards, data center personnel, and/or other appropriate personnel.	Observed the security desk at each INAP data centers to verify that data centers were monitored 24/7/365 by security guards, data center personnel, and/or other personnel.	No exceptions noted.
		INAP employs 24 hour video surveillance to monitor all entrances, exits, and other sensitive areas of its data centers. The video surveillance footage is retained for at least 90 days.	Observed video surveillance cameras at entrances, exits, and other sensitive areas to verify that entrances, exits, and sensitive areas of each INAP data center were monitored. Observed historical surveillance video footage to verify that recordings were retained for at least 90 days at each INAP data center.	No exceptions noted.
		INAP data center power and environmental conditions are monitored and reported via automated monitoring systems. INAP personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Observed the BMS monitoring and reporting system and alerts received by INAP personnel to verify that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
		INAP personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the incident log to verify that INAP personnel tracked data center power, environmental, and other incidents affecting data center availability. Inspected the NOC tickets for a sample of availability incidents to verify that availability related incidents were tracked, and escalated until resolution.	No exceptions noted.
		Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to verify that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		A smoke detection system is installed in each INAP data center to detect and alert data center personnel to the presence of a fire. Each critical smoke detection system is inspected and serviced at least annually to ensure effective operation.	Observed the smoke detection systems during virtual or on-site data center walkthroughs to verify that a smoke detection system was installed in each data center to detect and alert data center personnel to the presence of a fire. Inspected the most recent smoke detection system preventative maintenance report to verify that the smoke detection system was inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
		Multiple HVAC units control both temperature and humidity within each INAP data center, delivering redundant HVAC service throughout the data center. HVAC units are inspected and serviced at least annually to ensure effective operation.	Observed the HVAC units within each data center during virtual or on-site data center walkthroughs to verify that multiple HVAC units were utilized to control both temperature and humidity. Inspected the HVAC preventative maintenance reports to verify that HVAC units were inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
		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 each INAP data center. UPS systems are inspected and serviced at least annually to ensure effective operation.	Observed the UPS systems within each data center during virtual or on-site data center walkthroughs to verify that redundant UPS systems were utilized to provide temporary power in the event of a power failure and mitigate the risk of power surges impacting the data center infrastructure. Inspected the UPS preventative maintenance reports to verify that UPS systems were inspected and serviced at least annually to ensure effective operation.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 4	**Common Criteria Related to Monitoring Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Multiple diesel generators are in place to provide backup power in the event of a power outage at each INAP data center. Generators are inspected and serviced at least annually to ensure effective operation.	Observed the diesel generator systems within each data center during virtual or on-site data center walkthroughs to verify that multiple diesel generators were utilized to provide backup power in the event of a power outage. Inspected the backup generators preventative maintenance reports to verify that the generators were inspected and serviced during the review period to ensure effective operation.	No exceptions noted.
		The operating effectiveness of backup power systems at each INAP data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results to verify that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
		The Company performs an annual Cybersecurity Risk Assessment to identify risks and assess the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk assessment to verify that INAP identified risks and assessed risk mitigation controls on an annual basis. Inspected the cybersecurity risk register to verify that risk items and remediation plans were tracked until resolved.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Internal Audit independently assesses INAP's compliance with its SOC 2 and PCI objectives through the identification and assessment of risks and review of the controls that mitigate risks to those objectives. Additional entity level, IT, and operational controls are developed and/or updated, when necessary, to mitigate risks that threaten achievement of INAP's objectives. Control gaps and deficiencies identified during internal and external assessments are communicated to management and the board of directors as appropriate and tracked through resolution.	Inspected the risk and controls matrices to verify that Internal Audit assessed SOC 2 and PCI compliance, identified and assessed risk, and reviewed controls to mitigate risk. Inspected the risk and controls matrices to verify that Internal Audit developed and updated entity level, IT and operational control activities to mitigate risks that could threaten achievement of INAP's objectives. Inspected the control deficiency tracker and communications to management to verify that identified control gaps and deficiencies were communicated to management and the board of directors as needed and tracked through resolution.	No exceptions noted.
		The Company performs an annual Cybersecurity Risk Assessment to identify risks and assess the controls in place to mitigate those risks. Risk items and related treatment plans are added to the risk register and tracked until remediation.	Inspected the results of the most recent Cybersecurity Risk assessment to verify that INAP identified risks and assessed risk mitigation controls on an annual basis. Inspected the cybersecurity risk register to verify that risk items and remediation plans were tracked until resolved.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Human Resources policies and procedures are in place providing a framework for hiring, training, promoting, and compensating employees across the organization. An employment prescreening process is performed for new hires, which includes background, credit, and DMV checks (based on job requirements).	Observe the prescreening documentation for a sample of new hires to verify that Human Resources obtained background, credit, and/or DMV checks for each new hire as part of the employment prescreening process.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP has an annual objective setting process and employee evaluation process. During these periods, managers and employees discuss and assess expectations regarding performance; roles and responsibilities, including internal controls; ethics; integrity; and training needs. Human Resources tracks completion and results of the assessment procedure.	Inspected the performance evaluation template to verify that expectations regarding performance, ethics, integrity, and training needs were part of the objective setting and employee evaluation process. Inspected the current year's employee performance review tracking spreadsheet to verify that Human Resources tracked completion and results of the annual assessment.	No exceptions noted.
		The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management annually and available to employees on SharePoint.	Inspected INAP policies and procedures to verify that INAP maintained IT related policies and procedures, including Information Security, Change Management, and other operational and conduct policies, and that they were reviewed and approved by management annually. Inspected a screen shot of the policies and procedures published to the Company's SharePoint site to verify that the IT policies and procedures were available to employees.	No exceptions noted.
		Each INAP Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management on an annual basis.	Inspected the Data Center Operations Manual for each INAP data center to verify that each INAP Company controlled data centers had a Data Center Operations Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 5	**Common Criteria Related to Control Activities**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP's Network Operations Center (NOC) procedures are in place which are available to NOC personnel to provide guidance on responding to requests and issues. The NOC procedures are reviewed and approved by management on an annual basis.	Inspected INAP's NOC procedures to verify that the procedures were available to NOC personnel, included guidance for responding to requests and issues, and reviewed and approved by management on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Roles based access to applications ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	Inspected the user access listings for the in-scope systems to verify that privileges and authorizations were assigned based on the users' roles.	No exceptions noted.
		Access to the network and applications are restricted by requiring passwords or other system specific authentication control protocols. Password length, complexity, change, and account lockout requirements are established for systems in accordance with company policy. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected login screens for the network and applications to verify user authentication was required to access the system and applications. Inspected the Information Security Policy and network and application password and account lockout settings to verify that the systems were configured to enforce minimum password length, complexity, periodic password rotation, and account lockout requirements in accordance with policy. Inspected the policy exemptions for systems where implementation of password and account lockout policies was limited.	No exceptions noted.
		The Company has firewalls in place to limit access over the internet for internal corporate networks.	Inspected the network diagrams and firewall rules for a subset of the in-scope data centers to verify that firewalls were in place to limit access over the internet to corporate networks.	No exceptions noted.
		Connections via VPN tunnel between company locations are protected using encryption. Connections to applications via the internet are protected using encryption. VPN connections for user workstations outside the network require two factor authentication.	Inspected the web application TLS configurations to verify that connections via the internet were protected using encryption.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to applications, operating systems, and databases is properly approved by Human Resources, management, and/or authorized system owner.	Inspected the access approvals for a sample of new hires to verify that access to applications, operating systems, and databases was approved by Human Resources, management, and /or the authorized system owner.	No exceptions noted.
		Terminated employee system access is removed by IT in a timely manner.	Inspected the access removal ticket and Active Directory listing for a sample of terminated employees to verify that a system access was removed in a timely manner.	Exceptions noted on the terminated user system access removal process and documentation.
		For 3 of 37 terminated employees, system access was not removed in a timely manner. In addition, for 2 of 37 terminated employees, INAP could not provide the access termination tickets. Refer to Section V. Other Information Provided By Internap Holding LLC for Management's Response.		
		Application access, as well as database, and operating system privileged access, is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed privileged user access review to verify that management reviewed users' privileged access to application, database and operating system on an annual basis to ensure access is commensurate with job responsibilities.	No exceptions noted.
		User access to add, modify, and delete users in INAP's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspect the most recently performed keycard system reviews to verify that individuals with access to add, modify, and delete users in the keycard system were reviewed for appropriateness based on their job responsibilities on an annual basis.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		The customer contact authorization lists define the customer personnel authorized to access INAP data centers. User access to edit the customer contact authorization lists is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspected the most recently performed customer contact list reviews to verify that user access to edit the customer contact lists was reviewed for appropriateness based on their job responsibilities on an annual basis.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.	Roles based access to applications ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	Inspected the user access listings for the in-scope systems to verify that privileges and authorizations were assigned based on the users' roles.	No exceptions noted.
		Access to applications, operating systems, and databases is properly approved by Human Resources, management, and/or authorized system owner.	Inspected the access approvals for a sample of new hires to verify that access to applications, operating systems, and databases was approved by Human Resources, management, and /or the authorized system owner.	No exceptions noted.
		Terminated employee system access is removed by IT in a timely manner.	Inspected the access removal ticket and Active Directory listing for a sample of terminated employees to verify that a system access was removed in a timely manner.	Exceptions noted on the terminated user system access removal process and documentation.
		For 3 of 37 terminated employees, system access was not removed in a timely manner. In addition, for 2 of 37 terminated employees, INAP could not provide the access termination tickets. Refer to Section V. Other Information Provided By Internap Holding LLC for Management’s Response.		
		Application access, as well as database, and operating system privileged access, is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed privileged user access review to verify that management reviewed users' privileged access to applications, database and operating system on an annual basis to ensure access is commensurate with job responsibilities.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		User access to add, modify, and delete users in INAP's keycard system is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspect the most recently performed keycard system reviews to verify that individuals with access to add, modify, and delete users in the keycard system were reviewed for appropriateness based on their job responsibilities on an annual basis.	No exceptions noted.
		The customer contact authorization lists define the customer personnel authorized to access INAP data centers. User access to edit the customer contact authorization lists is reviewed for appropriateness based on job responsibilities on an annual basis.	Inspected the most recently performed customer contact list reviews to verify that user access to edit the customer contact lists was reviewed for appropriateness based on their job responsibilities on an annual basis.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	In order to gain physical access to INAP data centers, individuals must be validated via a combination of key card and/or biometric technology.	Observed successful and unsuccessful attempts to gain physical access to each data center to verify that employees and customers must be validated by keycard and/or biometric technology.	No exceptions noted.
		Customer equipment in INAP data centers is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.	Observed customer equipment segregated via locked cages or cabinets using a combination lock, badge reader, or physical key in each data center to ensure that customers could only access their own equipment.	No exceptions noted.
		For employees, contractors, and customers that are given permanent physical access badges to INAP data centers, access is properly approved during the onboarding process.	Inspected the INAP data center physical access approvals for a sample of new employees, contractors and customers with permanent access badges to verify that access was properly approved during the onboarding process.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Visitor access to INAP data centers is logged at the security desk. Visitors are easily distinguishable from onsite personnel based on the identification provided to visitors and/or personnel.	Observed data center visitor logs at each data center to verify that visitor access to INAP data centers was logged. Observed the visitor badges at each data center noting that visitors were easily distinguishable from onsite personnel badges.	Exception noted on the visitor badges at LAX014.
		LAX014 did not issue visitor badges due to COVID-19. Instead, visitors were identified by the absence of a badge since onsite personnel were still required to wear their badges. Refer to Section V. Other Information Provided By Internap Holding LLC for Management's Response.		
		Physical access to INAP data centers is revoked upon notification for terminated employees, contractors, and customers with permanent physical access badges.	Inspected the INAP data center physical access removal tickets for a sample of terminated employees, contractors and customers with permanent access badges to verify that access was revoked.	No exceptions noted.
		Quarterly audits are performed to validate the appropriateness of all employee, contractor, and customer physical access to INAP data centers. Third party service vendors of INAP are contacted periodically to verify the appropriateness of contractor physical access to data centers.	Inspected the results of quarterly physical access audits for a sample of quarters to verify that quarterly audits were performed to validate the appropriateness of employee, contractor, and customer physical access to the data centers. Inspected e-mails to verify that INAP's third party service vendors were contacted periodically to verify the appropriateness of contractor physical access to data centers.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The Company has firewalls in place to limit access over the internet for internal corporate networks.	Inspected the network diagrams and firewall rules for a subset of the in-scope data centers to verify that firewalls were in place to limit access over the internet to corporate networks.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Connections via VPN tunnel between company locations are protected using encryption. Connections to applications via the internet are protected using encryption. VPN connections for user workstations outside the network require two factor authentication.	Inspected the web application TLS configurations to verify that connections via the internet were protected using encryption.	No exceptions noted.
		Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		Employees have the capability to report potential phishing attempts and other issues to the CISO office. Information is provided via email to both alert and help educate employees when potential security issues are observed.	Inspected the phishing reporting configuration to verify that employees have the capability to report potential phishing attempts and other issues to the CISO office. Inspected examples of email alerting and informing employees when potential phishing attempts and other issues were observed.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Antivirus software is used on all in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected the antivirus software status of workstations and servers on the registered device listing to verify that antivirus software was installed on all servers and workstations. Inspected the antivirus settings to verify that antivirus software was configured to accept automatic updates and periodically scan for malware. Inspected the signed policy exceptions for each instance where system limitations prevented the installation of antivirus software to verify that signed policy exceptions were obtained.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Customer backups are made to non-removable storage media. Stored data is securely deleted based on an authorized cloud operations or customer request. When customers request that physical storage hardware be destroyed, this is accomplished securely by a third party vendor and a certificate of destruction delivered to the customer.	Inspected the List of Hardware Destruction Requests for a sample of data deletion requests to verify that stored data was deleted based on authorized cloud operations personnel or customer requests. Inspected evidence of destruction for a sample of customers who submitted requests to destroy storage hardware to verify that when hardware was destroyed, it was performed using a secure method and a certificate of destruction was delivered to the customer.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Normal IT changes must be reviewed and approved by the Change Advisory Board (CAB) and/or IT management before being implemented. Approvals and testing plans if applicable are documented within the ticketing system.	Inspected the IT change tickets for a sample of standard changes to verify that changes were reviewed and approved by the CAB and/or IT management before implementation and documented within the ticketing system when applicable.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 6	**Common Criteria Related to Logical and Physical Access Controls**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Application access, as well as database, and operating system privileged access, is reviewed at least annually by management to help ensure that access is commensurate with job responsibilities.	Inspected the most recently performed privileged user access review to verify that management reviewed users' privileged access to application, database and operating system on an annual basis to ensure access is commensurate with job responsibilities.	No exceptions noted.
		Antivirus software is used on all in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected the antivirus software status of workstations and servers on the registered device listing to verify that antivirus software was installed on all servers and workstations. Inspected the antivirus settings to verify that antivirus software was configured to accept automatic updates and periodically scan for malware. Inspected the signed policy exceptions for each instance where system limitations prevented the installation of antivirus software to verify that signed policy exceptions were obtained.	No exceptions noted.
		Vulnerability scans are performed at least quarterly for the internal corporate networks and identified vulnerabilities are assessed. Vulnerabilities are communicated to the owner of the IT asset and tracked by IT until remediation.	Inspected the vulnerability scan results for a sample of quarters to verify that vulnerability scans of the internal corporate network were performed at least quarterly and identified vulnerabilities were assessed. Inspected the remediation tickets for a sample of vulnerabilities identified during the quarterly vulnerability scans to verify that vulnerabilities were communicated to the owner of the IT asset and tracked by IT until remediation.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		Antivirus software is used on all in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected the antivirus software status of workstations and servers on the registered device listing to verify that antivirus software was installed on all servers and workstations. Inspected the antivirus settings to verify that antivirus software was configured to accept automatic updates and periodically scan for malware. Inspected the signed policy exceptions for each instance where system limitations prevented the installation of antivirus software to verify that signed policy exceptions were obtained.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Vulnerability scans are performed at least quarterly for the internal corporate networks and identified vulnerabilities are assessed. Vulnerabilities are communicated to the owner of the IT asset and tracked by IT until remediation.	Inspected the vulnerability scan results for a sample of quarters to verify that vulnerability scans of the internal corporate network were performed at least quarterly and identified vulnerabilities were assessed. Inspected the remediation tickets for a sample of vulnerabilities identified during the quarterly vulnerability scans to verify that vulnerabilities were communicated to the owner of the IT asset and tracked by IT until remediation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Antivirus software is used on all in scope workstations and servers and configured to accept automatic software updates and periodically scan for malware. In instances where system limitations prevent implementation, policy exemptions are documented.	Inspected the antivirus software status of workstations and servers on the registered device listing to verify that antivirus software was installed on all servers and workstations. Inspected the antivirus settings to verify that antivirus software was configured to accept automatic updates and periodically scan for malware. Inspected the signed policy exceptions for each instance where system limitations prevented the installation of antivirus software to verify that signed policy exceptions were obtained.	No exceptions noted.
		Vulnerability scans are performed at least quarterly for the internal corporate networks and identified vulnerabilities are assessed. Vulnerabilities are communicated to the owner of the IT asset and tracked by IT until remediation.	Inspected the vulnerability scan results for a sample of quarters to verify that vulnerability scans of the internal corporate network were performed at least quarterly and identified vulnerabilities were assessed. Inspected the remediation tickets for a sample of vulnerabilities identified during the quarterly vulnerability scans to verify that vulnerabilities were communicated to the owner of the IT asset and tracked by IT until remediation.	No exceptions noted.
		INAP data center power and environmental conditions are monitored and reported via automated monitoring systems. INAP personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Observed the BMS monitoring and reporting system and alerts received by INAP personnel to verify that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the incident log to verify that INAP personnel tracked data center power, environmental, and other incidents affecting data center availability. Inspected the NOC tickets for a sample of availability incidents to verify that availability related incidents were tracked, and escalated until resolution.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected the cybersecurity Incident Report for a sample of cybersecurity incidents to verify that an Incident Report was prepared by IT and/or CISO office, included a root cause analysis and corrective action plan, when applicable, and were implemented when deemed necessary by management.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the Event Reports for a sample of serious incidents to verify that an Event Report was prepared by Data Center Operations personnel and it included a root cause analysis and corrective action plan, when necessary, for each serious incident.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO and/or network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	Observed the network monitoring tool in place to detect unauthorized network access during a virtual meeting with CISO and a network engineer. Inspected the alert configuration(s) and sample of network security alerts to verify that critical alerts were sent real time to the CISO and/or network engineering group for follow up and resolution. Inspected examples of network security issue tickets to verify that issues and incidents were escalated as necessary and tracked until resolution.	No exceptions noted.
		An Incident Response Policy and Incident Response Plan are documented and in place. These are reviewed and approved by management annually and are available to employees on SharePoint.	Inspected the Incident Response Policy and Incident Response Plan to verify they were documented, and reviewed and approved by management annually. Inspected a screen shot of the Incident Response Policy and Incident Response Plan published to the Company's SharePoint site to verify that the Incident Response Policy and Plan were available to employees.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected the cybersecurity Incident Report for a sample of cybersecurity incidents to verify that an Incident Report was prepared by IT and/or CISO office, included a root cause analysis and corrective action plan, when applicable, and were implemented when deemed necessary by management.	No exceptions noted.
		Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the Event Reports for a sample of serious incidents to verify that an Event Report was prepared by Data Center Operations personnel and it included a root cause analysis and corrective action plan, when necessary, for each serious incident.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Cybersecurity incidents are analyzed to identify the root cause. Recovery actions are taken as applicable, corrective action plans are put into place and the incident response plan and recovery procedures are updated as necessary to prevent, detect and respond to future cybersecurity incidents.	Inspected the cybersecurity Incident Report for a sample of cybersecurity incidents to verify that an Incident Report was prepared by IT and/or CISO office, included a root cause analysis and corrective action plan, when applicable, and were implemented when deemed necessary by management.	No exceptions noted.
		Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the Event Reports for a sample of serious incidents to verify that an Event Report was prepared by Data Center Operations personnel and it included a root cause analysis and corrective action plan, when necessary, for each serious incident.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 7	**Common Criteria Related to Systems Operations**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		The Incident Response Team is trained annually. The Incident Response Plan is tested at least annually and feedback from the test is incorporated into the Plan, if applicable.	Inspected training documentation to verify that the Incident Response Team was trained on Incident Response Plan annually. Inspected the Incident Response Plan test results to verify that the Incident Response Plan was tested at least annually and feedback was incorporated into the Plan when applicable.	No exceptions noted.
		The company's Business Continuity Plan (BCP) is reviewed and updated at least annually. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to verify that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated at least annually. Inspected the results of the most recently performed BCP test to verify that BCP testing was conducted annually and updates to the BCP were considered based on the test results.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC 8	**Common Criteria Related to Change Management**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The Company maintains policies and procedures pertaining to IT, including Information Security, Change Management, and other policies for operations and conduct. These are reviewed and approved by management annually and available to employees on SharePoint.	Inspected INAP policies and procedures to verify that INAP maintained IT related policies and procedures, including Information Security, Change Management, and other operational and conduct policies, and that they were reviewed and approved by management annually. Inspected a screen shot of the policies and procedures published to the Company's SharePoint site to verify that the IT policies and procedures were available to employees.	No exceptions noted.
		Normal IT changes must be reviewed and approved by the Change Advisory Board (CAB) and/or IT management before being implemented. Approvals and testing plans if applicable are documented within the ticketing system.	Inspected the IT change tickets for a sample of standard changes to verify that changes were reviewed and approved by the CAB and/or IT management before implementation and documented within the ticketing system when applicable.	No exceptions noted.
		The Company has in place a Change Management process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	Inspected the data center infrastructure change tickets/forms for a sample of infrastructure changes to verify that the INAP had a Change Management process in place to ensure all scheduled maintenance and other data center implementations / modifications were properly documented and authorized to assure minimal impact to customers. Inspected the customer notifications for a sample of scheduled maintenance or other changes that could affect customer availability to verify that customers were notified in advance.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC9	**Common Criteria Related to Risk Mitigation**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's Business Continuity Plan (BCP) is reviewed and updated at least annually. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to verify that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated at least annually. Inspected the results of the most recently performed BCP test to verify that BCP testing was conducted annually and updates to the BCP were considered based on the test results.	No exceptions noted.
		Insurance policies are obtained to offset the financial impact of loss events that would potentially impair the company in achieving its objectives. Property/casualty insurance is obtained for INAP flagship data centers and cybersecurity insurance is obtained for the company as a whole.	Inspected the insurance policies to verify that property/casualty insurance was obtained for INAP's flagship data centers. Inspected the cybersecurity insurance policy to verify that cybersecurity insurance was obtained for INAP as a whole.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The scope of services agreed to with new vendor service providers which could impact the security and availability of INAP data centers, as well as any compliance or security requirements and SLAs that the vendor must adhere to, are documented in contractual agreements with the vendor.	Inspected the contractual agreements for a sample of vendors to verify that the scope and any service, compliance or security requirements were documented in the vendor contractual agreements.	No exceptions noted.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES CATEGORIES				
CC9	**Common Criteria Related to Risk Mitigation**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		Formalized vendor risk assessments are performed for new vendor service providers that could impact the security and availability of INAP data centers. Risks considered include, as applicable, (1) any access a vendor will have to facilities and data, including access to confidential or restricted data, (2) how INAP data will be transmitted, processed, or stored by the vendor, (3) whether the vendor will share such data with other third parties, (4) whether the vendor will be given access to INAP systems, and other risk factors.	Inspected the vendor risks assessments for a sample of new vendors to verify that a vendor risk assessment was performed and considered security and availability related risks such as vendor access rights; data exchanges, transmissions, processing and storage; and access to INAP systems.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A	**Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Data center power and cooling capacity reports are prepared at least monthly to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	Inspected the data center power and cooling capacity reports for a sample of months to verify that data center power and cooling capacity reports were prepared to assist Data Center Operations management maintain, monitor, and evaluate power and cooling capacity needs.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The company's Business Continuity Plan (BCP) is reviewed and updated at least annually. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to verify that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated at least annually. Inspected the results of the most recently performed BCP test to verify that BCP testing was conducted annually and updates to the BCP were considered based on the test results.	No exceptions noted.
		Each INAP Company controlled data center has a detailed Data Center Operations Manual which is available to Data Center Operations personnel and includes emergency procedures, contact information, and data center equipment details, monitoring and/or maintenance requirements. Each Data Center Operations Manual is reviewed and approved by management on an annual basis.	Inspected the Data Center Operations Manual for each INAP data center to verify that each INAP Company controlled data centers had a Data Center Operations Manual available to Data Center Operations personnel, procedures were documented, internal control requirements were specified, and the Manual was reviewed and approved by management on an annual basis	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A	**Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		INAP data center power and environmental conditions are monitored and reported via automated monitoring systems. INAP personnel receive and monitor alerts regarding the real-time status of power, HVAC, temperature, and fire detection/suppression conditions.	Observed the BMS monitoring and reporting system and alerts received by INAP personnel to verify that data center power and environmental conditions were monitored and reported via automated monitoring systems.	No exceptions noted.
		INAP personnel track data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	Inspected the incident log to verify that INAP personnel tracked data center power, environmental, and other incidents affecting data center availability. Inspected the NOC tickets for a sample of availability incidents to verify that availability related incidents were tracked, and escalated until resolution.	No exceptions noted.
		Significant incidents affecting data center physical security and/or availability are analyzed to identify the root cause. Recovery actions are taken as applicable and corrective action plans are put into place, as necessary, to prevent, detect and respond to future incidents.	Inspected the Event Reports for a sample of serious incidents to verify that an Event Report was prepared by Data Center Operations personnel and it included a root cause analysis and corrective action plan, when necessary, for each serious incident.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A	**Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		A smoke detection system is installed in each INAP data center to detect and alert data center personnel to the presence of a fire. Each critical smoke detection system is inspected and serviced at least annually to ensure effective operation.	Observed the smoke detection systems during virtual or on-site data center walkthroughs to verify that a smoke detection system was installed in each data center to detect and alert data center personnel to the presence of a fire. Inspected the most recent smoke detection system preventative maintenance report to verify that the smoke detection system was inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
		Each INAP 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. Each critical 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.	Observed the pre-action, dry pipe sprinkler fire suppression systems and fire extinguishers during virtual or on-site data center walkthroughs to verify the data centers were protected against risk of fire. Inspected the fire suppression system and fire extinguisher maintenance reports to verify that the data centers' fire suppression systems and fire extinguishers were serviced at least annually to ensure effective operation.	No exceptions noted.
		Multiple HVAC units control both temperature and humidity within each INAP data center, delivering redundant HVAC service throughout the data center. HVAC units are inspected and serviced at least annually to ensure effective operation.	Observed the HVAC units within each data center during virtual or on-site data center walkthroughs to verify that multiple HVAC units were utilized to control both temperature and humidity. Inspected the HVAC preventative maintenance reports to verify that HVAC units were inspected and serviced at least annually to ensure effective operation.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A	**Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
		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 each INAP data center. UPS systems are inspected and serviced at least annually to ensure effective operation.	Observed the UPS systems within each data center during virtual or on-site data center walkthroughs to verify that redundant UPS systems were utilized to provide temporary power in the event of a power failure and mitigate the risk of power surges impacting the data center infrastructure. Inspected the UPS preventative maintenance reports to verify that UPS systems were inspected and serviced at least annually to ensure effective operation.	No exceptions noted.
		Multiple diesel generators are in place to provide backup power in the event of a power outage at each INAP data center. Generators are inspected and serviced at least annually to ensure effective operation.	Observed the diesel generator systems within each data center during virtual or on-site data center walkthroughs to verify that multiple diesel generators were utilized to provide backup power in the event of a power outage. Inspected the backup generators preventative maintenance reports to verify that the generators were inspected and serviced during the review period to ensure effective operation.	No exceptions noted.
		The operating effectiveness of backup power systems at each INAP data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results to verify that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A	**Availability**			
Criteria		**Service Organization Control Activity**	**Test Performed by the Service Auditor**	**Test Results**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's Business Continuity Plan (BCP) is reviewed and updated at least annually. As part of the BCP, threats that could impair the availability of data centers are identified and ranked by overall risk (determined by likelihood and impact). Annual testing of the BCP is conducted and updates to the Plan are considered based on test results.	Inspected the BCP to verify that the BCP considered environmental threats that could impair data center availability, risks were ranked, and the BCP was reviewed and updated at least annually. Inspected the results of the most recently performed BCP test to verify that BCP testing was conducted annually and updates to the BCP were considered based on the test results.	No exceptions noted.
		The operating effectiveness of backup power systems at each INAP data center are confirmed at least annually, through load bank testing and/or other methods.	Inspected the most recently performed backup power system test results to verify that the operating effectiveness of backup power systems were tested at least annually through load bank testing and/or other methods.	No exceptions noted.

V. OTHER INFORMATION PROVIDED BY INTERNAP HOLDING LLC

In addition to the information in Section IV, Information Provided By The Independent Service Auditors, the following additional information is being provided by INAP management as it may be relevant to the reader to obtain a better understanding of INAP's exceptions. The following Management's Responses to the exceptions noted in Section IV are not within the scope of this examination and have not been audited.

<table>
<tr><th>Service Organization Control Activity</th><th>Test Performed by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>Terminated employee system access is removed by IT in a timely manner.</td><td>Inspected the access removal ticket and Active Directory listing for a sample of terminated employees to verify that a system access was removed in a timely manner.</td><td>Exceptions noted on the terminated user system access removal process and documentation.</td></tr>
<tr><td colspan="3">For 3 of 37 terminated employees, system access was not removed in a timely manner. In addition, for 2 of 37 terminated employees, INAP could not provide the access termination tickets.

Management's Response:
The impact of these employees retaining active accounts beyond their termination date was mitigated through the shipping and/or collection of their company provided laptops. Access to production systems in scope requires onsite and/or VPN access which requires two factor authentication: (1) password and (2) OTP token which can only be generated from the user's company provided laptop. The employee's company provided laptop is required to access the INAP network.
Additional monitoring of the terminated employee access removal process is being performed by the Office of the CISO and by Internal Audit.
As of Q3 2020, quarterly audits by the CISO and/or Internal Audit are being performed. A weekly review has been implemented as of Q1 2021, whereby the Office of the CISO and/or Internal Audit compare recorded employee terminations in ADP and ensure access is revoked in a timely manner.</td></tr>
</table>

<table>
<tr><th>Service Organization Control Activity</th><th>Test Performed by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>Visitor access to INAP data centers is logged at the security desk. Visitors are easily distinguishable from onsite personnel based on the identification provided to visitors and/or personnel.</td><td>Observed data center visitor logs at each data center to verify that visitor access to INAP data centers was logged.
Observed the visitor badges at each data center noting that visitors were easily distinguishable from onsite personnel badges.</td><td>Exception noted on the visitor badges at LAX014.</td></tr>
<tr><td colspan="3">LAX014 did not issue visitor badges due to COVID-19. Instead, visitors were identified by the absence of a badge since onsite personnel were still required to wear their badges.

<b>Management’s Response:</b>
At the beginning of the COVID-19 pandemic, issuance of visitor nametags was temporarily discontinued at LAX014 as a precaution against the spread of the virus. As of August 31, 2020, the procedure to issue visitor nametags has been communicated to, acknowledged, and implemented by the LAX014 data center management team. Precautions in line with CDC guidance such as hand sanitizer, COVID-19 screening, and updated COVID-19 health procedures are in place to appropriately mitigate this risk of exposure to COVID-19.</td></tr>
</table>