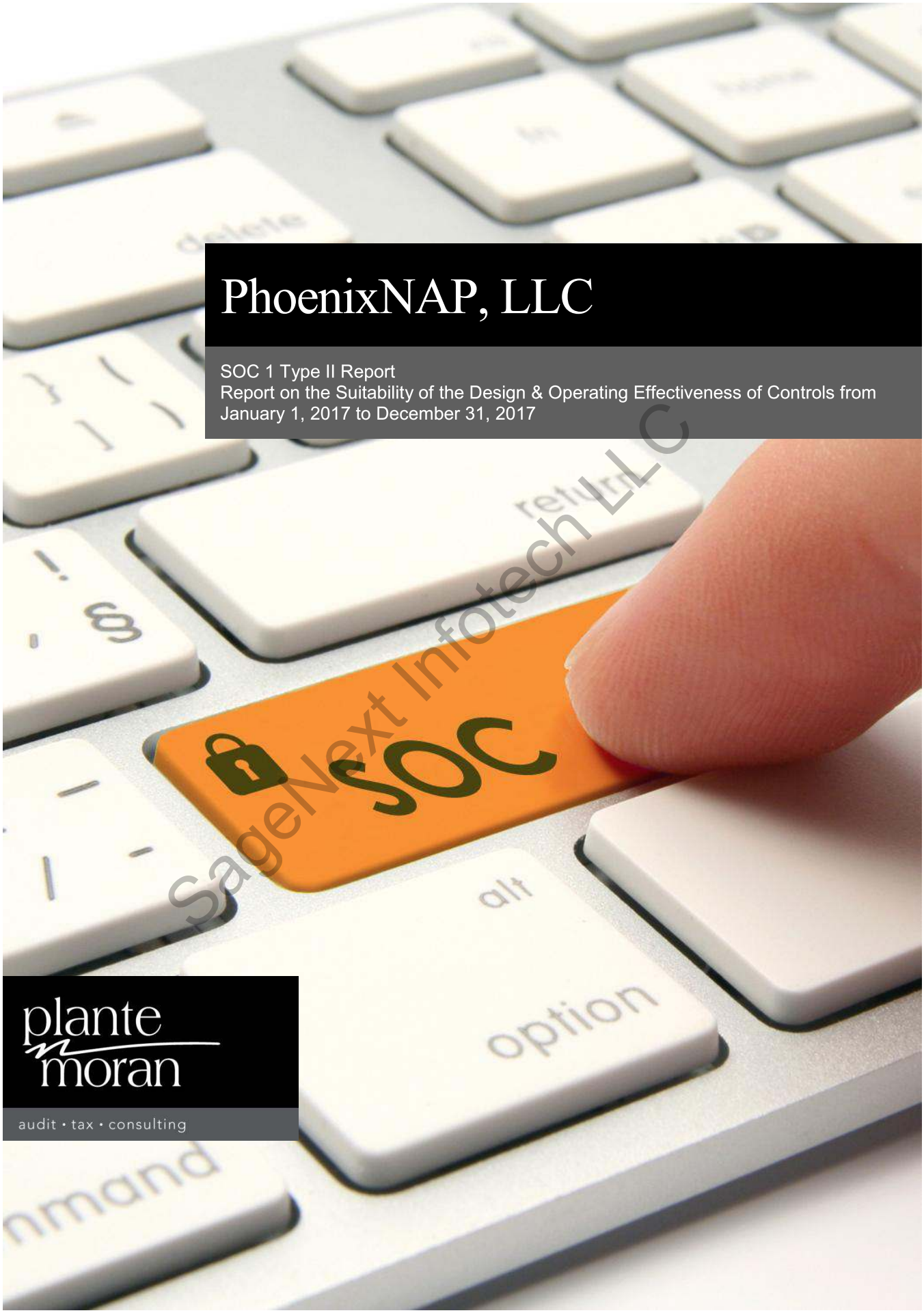
PhoenixNAP, LLC

SOC 1 Type II Report
Report on the Suitability of the Design & Operating Effectiveness of Controls from January 1, 2017 to December 31, 2017



plante moran

audit • tax • consulting

Contents

plante moran

Plante & Moran, PLLC
10 South Riverside Plaza
9th floor
Chicago, IL 60606
Tel: 312.207.1040
Fax: 312.207.1066
plantemoran.com

Section I: Independent Service Auditor's Report

To: Management of PhoenixNAP, LLC
Phoenix, Arizona

Scope

We have examined PhoenixNAP, LLC's ("PhoenixNAP" or "the Company") description of its Cloud Services Information Technology General Controls System entitled "Description of PhoenixNAP, LLC's "PhoenixNAP, LLC's Description of its Cloud Services Information Technology General Controls System for the period January 1, 2017 to December 31, 2017" applicable to the cloud and colocation platform for users of the system throughout the period January 1, 2017 to December 31, 2017 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "PhoenixNAP, LLC's Assertion". The controls and control objectives included in the description are those that management of PhoenixNAP believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Cloud Services Information Technology General Controls System that are not likely to be relevant to user entities' internal control over financial reporting.

PhoenixNAP uses subservice organizations for data center colocation services. A list of these subservice organizations is provided in the description of the system. The description of the system in Section III and the control objectives and related controls listed in Section IV of this report, include only the control objectives and related controls of PhoenixNAP and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls at the subservice organizations assumed in the design of PhoenixNAP's controls are suitably designed and operating effectively, along with related controls at PhoenixNAP. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of PhoenixNAP's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

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 the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2017 to December 31, 2017. 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 the service organization's controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertions.

Inherent Limitations

PhoenixNAP's description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements of the Cloud Services Information Technology General Controls System. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of our tests are presented in Section IV of this report. The scope of our engagement did not include tests to determine whether control activities not listed in Section IV were achieved; accordingly, we express no opinion on the achievement of control objectives or control activities not included in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in PhoenixNAP's assertion

a. the description fairly presents the Cloud Services Information Technology General Controls System used by PhoenixNAP for the cloud and colocation platform for user entities of the system that was designed and implemented throughout the period January 1, 2017 to December 31, 2017,

b. the controls of PhoenixNAP related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2017 to December 31, 2017 and subservice organizations and user entities applied the complementary controls assumed in the design of PhoenixNAP's controls throughout the period January 1, 2017 to December 31, 2017,

c. the controls that we tested, which were those necessary to provide reasonable assurance that the control objectives were achieved operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2017 to December 31, 2017 if complementary subservice organization and user entity controls assumed in the design of PhoenixNAP's controls operated effectively throughout the period January 1, 2017 to December 31, 2017.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of PhoenixNAP, user entities of PhoenixNAP's Cloud Services Information Technology General Controls System during some or all of the period January 1, 2017 to December 31, 2017 and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than those specified parties.

Plante & Moran, PLLC

July 5, 2018
Chicago, Illinois

PhoenixNAP®
2353 West University Drive
Tempe, Arizona 85281
1.877.749.2656

July 5, 2018

Plante & Moran, PLLC
10 South Riverside Plaza
Chicago, Illinois 60606

To Service Auditors:

We have prepared the description of PhoenixNAP, LLC's ("PhoenixNAP" or "the Company") Cloud Services Information Technology General Controls System entitled "PhoenixNAP, LLC's Description of its Cloud Services Information Technology General Controls System for the Period January 1, 2017 to December 31, 2017" for the cloud and colocation platform for user entities of the system during some or all of the period January 1, 2017 to December 31, 2017 (description), and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

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

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

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

a. The description fairly presents the Cloud Services Information Technology General Controls System made available to user entities of the system Cloud Services Information Technology General Controls System during some or all of the period January 1, 2017 to December 31, 2017 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable
      1) the types of services provided;
      2) the procedures, within both automated and manual systems, by which those services provided are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;
      3) how the system captures and addresses significant events and conditions other than transactions;
      4) the process used to prepare reports and other information for user entities;

PhoenixNAP®
2353 West University Drive
Tempe, Arizona 85281
1.877.749.2656

5) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
6) the specified control objectives and controls designed to achieve those objectives including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls, and control objectives that are specified by law, regulation, or another party; and
7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided to user entities of the system.

ii. relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Cloud Services Information Technology General Controls System that each individual user entity of the system and its auditor may consider important in its own particular environment.

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

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

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

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

Very truly yours,

Steven Freeman, Director of Information Security

Section III: PhoenixNAP, LLC's Description of its Cloud Services Information Technology General Controls System for the Period January 1, 2017 to December 31, 2017

A. OVERVIEW OF OPERATIONS

Organization Background

PhoenixNAP (or "the Company") is a privately owned company headquartered in Phoenix, Arizona with data center operations owned and operated by PhoenixNAP in Phoenix, Arizona and other data center operations in facilities owned and operated by third parties in Ashburn, Virginia; Atlanta, Georgia; Amsterdam, Netherlands; Belgrade, Serbia; and Singapore (collectively, "colocated facilities"). PhoenixNAP provides services to more than 2,000 customers worldwide.

PhoenixNAP's suite of Infrastructure as a Service (IaaS) offerings provides hardware, networking, and platform support for clients to manage their own infrastructure environments.

PhoenixNAP provides a full suite of IT and Data Center services for its clients including colocation, hardware leasing, cloud servicing, availability, disaster recovery and security.

B. SCOPE OF THIS REPORT

Scope

PhoenixNAP's Cloud Services Information Technology General Controls System addressed within this report includes the following servers for the period from January 1, 2017 to December 31, 2017 and does not report on other service aspects of PhoenixNAP:

- Infrastructure as a service (IAAS): Public Cloud
- Infrastructure as a service (IAAS): Virtual Private Cloud
- Infrastructure as a service (IAAS) Managed Private Cloud
- Colocation Services

Changes in the internal control environment

The description of key control activities included in this report have been revised to describe the key control activities that are embedded into PhoenixNAP's Cloud Services Information Technology General Controls System, which may be different than internal controls reported on in prior Service Organization Control reports.

Subsequent Events

PhoenixNAP is not aware of any relevant events that occurred subsequent to December 31, 2017 through the date of the service auditor's report that would have a significant effect on its assertion in Section II.

C. SUMMARY OF CLOUD SERVICES INFORMATION TECHNOLOGY GENERAL CONTROLS SYSTEM

PhoenixNAP provides users of its Cloud Services Information Technology General Controls System a variety of options for managed cloud infrastructures. Each cloud environment is built on a VMware based virtual environment with vCenter hypervisors for management of each distinct environment. Nexenta and Hewlett Packard Enterprise Nimble Storage appliances are used as storage arrays. All servers are managed by PhoenixNAP employees located in offices and facilities throughout the world. Virtual Private Cloud and Managed Private Cloud users are able to establish performance and bandwidth requirements that PhoenixNAP's team manages and monitors to ensure minimum performance and service level thresholds are met.

The Cloud Services Information Technology General Controls System is provided by PhoenixNAP, using its state of the art data center, which includes physical and environmental protection features, and the colocation subservice organizations described below. The data center is a carrier neutral facility with multiple internet lines for connectivity and redundancy. Clients and colocation service users are able to select their desired internet service provider(s) for internet connectivity. PhoenixNAP utilizes a proprietary combination of internet service providers for its cloud services environment and monitors availability metrics for continuous connectivity and uptime.

An online portal is available for clients to access, monitor, and manage their virtual instances within the Cloud Services Information Technology General Controls System. The online portal also acts as a means for communicating issues and submitting incidents to the PhoenixNAP team for troubleshooting.

PhoenixNAP has designated portions of its Phoenix data center for colocation services. Users of PhoenixNAP's colocation service provide the hardware and infrastructure to be housed in PhoenixNAP's data center and leverages the physical security, environmental protection controls, and/or internet connectivity services of PhoenixNAP.

PhoenixNAP has physically segregated its corporate environment from its cloud services network infrastructure to enhance segregation of duties and reduce the risk of unauthorized access to the Cloud Services Information Technology General Controls System.

D. SUBSERVICE ORGANIZATIONS

PhoenixNAP uses subservice organizations to achieve operating efficiency. The Company periodically reviews the quality of the subservice organizations' performance. Reports on control environments for the third party data centers are reviewed on an annual basis by the security team. The following are the subservice organizations (collectively, "colocated facilities") used by PhoenixNAP:

- Zayo Group, LLC.: Colocation data center for Ashburn, Virginia
- NationalNet, Inc.: Colocation data center for Atlanta, Georgia
- EvoSwitch Netherlands B.V.: Colocation data center for Amsterdam, Netherlands
- Absolut Solutions: Colocation data center for Belgrade, Serbia
- Telstra: Colocation data center for Singapore

The physical and environmental controls provided by the colocated facilities are not included within the scope of this report. PhoenixNAP has considered the controls in place at each location and monitors them through periodic review of a SOC 1 Type 2 report obtained from each colocation subservice organization. Reviews of the SOC 1 Type 2 report include a comparison of PhoenixNAP's internal control environment with the specified user entity controls to determine whether gaps in controls are present.

The following controls are expected to be implemented at the colocated facilities:

Expected Controls to be Implemented by the Subservice Organization	Related Control Objective
All entrances to facilities are locked and access is properly restricted. A user access review of individuals with access to facilities is performed.	Control objective 3 – Physical Security
Firewall and IDS are in place and properly monitored. Scheduled backups are monitored for completeness. Monitoring for system performance and availability is performed on a periodic basis.	Control objective 4 – Systems Security and Monitoring
Incident management policies and procedures are defined for incident handling and breach management.	Control objective 4 – Systems Security and Monitoring
Hardware and network performance monitoring is performed on a periodic basis and administrators are notified of any issues.	Control objective 4 – Systems Security and Monitoring
The following controls are maintained for each data center: • Equipment kept on racks in data center • Smoke and fire detection system • Fire suppression system • Fire extinguishers • Dedicated A/C • UPS in place and tested at least quarterly • Generator in place and tested at least quarterly Environmental monitoring software exists and alerting is in place. Business continuity and disaster recovery plans exist and are updated at least annually.	Control objective 6 – Environmental

E. CONTROL OBJECTIVES AND RELATED CONTROLS

The control objectives and related controls are included in Section IV of this report to eliminate the redundancy that would result from listing them in this section and repeating them in Section IV. Although the control objectives and related controls are presented in Section IV, they are an integral part of PhoenixNAP's description of system.

F. OVERVIEW OF COMPANY-LEVEL INTERNAL CONTROL

Control Environment

Organizational Structure

PhoenixNAP's operations are overseen under the direction of the president and the board of directors. The Company is structured into four primary functional areas:

- Information Technology
  - Network operations and Engineering
  - Cloud Operations and Engineering
  - Systems Engineering
  - Information Security
- Administration
- Customer Service
- Data Center Operations/ Critical Environment Department

Organizational structure and reporting lines have been established to facilitate the flow of information to appropriate people in a timely manner and are depicted in the Company's organization chart. The organization chart is updated periodically to reflect changes. Roles and responsibilities are appropriately segregated based on functional requirements. Separation of duties exists and is specified in employee job descriptions.

The board of directors of PhoenixNAP exercises oversight responsibility related to internal control. The board members are involved in all significant business decisions. The board of directors meets informally almost daily and formally on an annual basis.

Executive management consists of the President, Chief Operations Officer (COO), Chief Financial Officer (CFO), Chief Legal Officer (CLO), Executive Vice President of Implementations, and Executive Vice President of Products. Executive management is responsible for making decisions on the overall vision and direction of the Company, including technology and security. Senior management are responsible for managing the operational, administrative, and engineering teams that handle the day to day operations of the Company.

PhoenixNAP also has external accounting and law firms that support annual filings and provide accounting, tax, and legal advice.

Integrity, Ethical Values, and Human Resources

There is an established "tone at the top," including hands-on executive involvement and continuous communication with staff regarding the Company's responsibility to uphold the highest levels of integrity in conducting both PhoenixNAP and customer affairs. This tone is communicated and practiced by executives and supervisors throughout the Company. The importance of high ethics and internal control is discussed with newly hired employees during orientation. PhoenixNAP requires each employee to sign an acknowledgement of their responsibilities for IT security and customer data protection.

Management has established human resource (HR) practices that demonstrate its commitment to integrity, ethical behavior, and competence. PhoenixNAP has developed an Employee Handbook, which includes policies that address acceptable business practices, conflicts of interest, and expected standards of ethical behavior. These policies are provided to all new employees and are available on the Company's intranet.

Management has a formal hiring and training process for all new employees, which is designed to ensure that each new employee is qualified to meet necessary requirements for job functions and roles. Hiring policies include minimum education and experience requirements, background checks, reference checks, and the execution of confidentiality statements. Background checks are performed for prospective employees, when permitted by local law and regulation, prior to the date of hire. Reference checks are performed when background checks are not permitted.

The board of directors review the compensation of members of executive management to ensure that pay is commensurate with responsibilities and incentive compensation is aligned with strategic objectives of the Company.

Management's Philosophy and Operating Style

Executive management holds regular meetings with personnel to maintain contact with and consistently emphasize appropriate behavior. During these meetings, management demonstrates attitudes and actions reflecting a sound control environment and commitment to ethical values.

Authority and Responsibility

All positions have written job descriptions including education and experience requirements and formally assigned authority and responsibility, which are provided to all PhoenixNAP employees on the Company intranet. Job descriptions include specific reference to internal control responsibilities, as applicable.

The Information Security Program establishes management's responsibility for all aspects of information security and authorizes management to delegate responsibilities to the Information Security Officer (ISO). The ISO is responsible for the design, operations, and monitoring of the Company's security and control environment. The Information Security Program is reviewed and approved annually by executive management.

All significant agreements and contracts, including those affecting information security, are reviewed and approved by executive management prior to being executed.

Commitment to Competence

Employees are evaluated annually on their job performance and fulfillment of company objectives and expectations by their supervisors. Disciplinary action procedures have been designed to provide managers with a process for communicating areas of improvements to employees. Employee performance along with compliance to company polices and expected behaviors are monitored on a continuous basis by supervisors. Formal communications and notifications are sent to employees and human resources when employees have exhibited noncompliance with company policies or expected behaviors.

Risk Assessment Process

PhoenixNAP has defined a risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the applicable tolerances. Responsibility for the risk assessment has been assigned to the ISO and a complete review of the Company risk assessment takes place at least annually.

During the annual risk assessment and management process, personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update identified potential threats to control objectives. Control activities are implemented at the conclusion of the risk assessment process.

Information and Communication Systems

Internal User Communications

PhoenixNAP has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities regarding customer services and internal control and to ensure that significant events are communicated in a timely manner. These methods include formal job descriptions, orientation for newly hired employees, a Company intranet, weekly forums and the use of electronic mail messages to communicate time-sensitive messages and information. The intranet provides access to Company announcements, policies and procedures, and executive emails.

Documented policies over ethical conduct, protection of information security, the employee handbook and statements of confidentiality and privacy practices are acknowledged at time of hire. Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints are published and available on the intranet.

Training programs have been developed to communicate and ensure employees are aware of their responsibilities for protection of the PhoenixNAP environment. Employees are required to attend security training on an annual basis.

External User Communications

PhoenixNAP has also implemented various methods of communication to ensure that user organizations understand the role and responsibilities of PhoenixNAP with respect to customer service and to ensure that significant events are communicated to users in a timely manner. These methods include PhoenixNAP's use of formal contracts that address the scope of services to be provided and the responsibilities of PhoenixNAP under the contracts. PhoenixNAP's security and availability commitments regarding the Cloud Services Information Technology General Controls System are included in the master services agreements (MSA) and customer-specific service level agreements (SLA). Additionally, a description of the Cloud Services Information Technology General Controls System and services provided by PhoenixNAP is made available to external users on a customer-facing website. Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are communicated to clients during the onboarding process.

Customer Support staff are responsible for maintaining customer relationships and communicating pertinent matters to customers. Customers are also encouraged to communicate questions and problems to the Company. Such matters are logged and tracked until resolved.

Monitoring

PhoenixNAP's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. Executive management, together with external contract auditors, assessors, and consultants perform ongoing audit functions to evaluate the internal control of PhoenixNAP. PhoenixNAP performs periodic evaluations of network, server and infrastructure availability, problem ticket resolution, and open items to determine whether services are continuously provided in a consistent, high-availability manner.

G. OVERVIEW OF SYSTEM LEVEL CONTROLS

Network Security

The Company's cloud network infrastructure is logically segmented between the hosting environment and the management infrastructure environment. The cloud network infrastructure includes the hypervisors and virtual machines where client instances are located. The management infrastructure environment includes servers, appliances, and tools for monitoring and managing the cloud network infrastructure.

Access to the management infrastructure environment is restricted to PhoenixNAP personnel and requires access through a bastion host. Dual factor authentication is required to access the bastion host. A web server in the management infrastructure environment hosts the PhoenixNAP portal, which allows clients to manage and monitor their instances in the public or private cloud. Connectivity to the PhoenixNAP portal is encrypted.

Firewalls are in place to monitor and block unauthorized internet-facing traffic to each environment. Virtual firewall capabilities are provided to clients and users of the Cloud Services Information Technology General Controls System. Clients are responsible for the management and monitoring of virtual firewalls within each hosted instance.

Local administrator rights on individual workstations are restricted to authorized personnel to limit the ability to install software. Antivirus software is installed on workstations, laptops, and servers. Scheduled scans take place on a weekly basis and members of the Information Security Team are notified when malware and threats are detected. Antivirus software is configured to receive updated virus signature definitions on a daily basis. The Network Operations Team receives a report of devices that have not been updated in 30 days and follows up on the devices. Updates and patches for PhoenixNAP systems are applied on a quarterly basis.

Logical Access

Unique user IDs and passwords are required to access the Company's cloud network infrastructure and management infrastructure environments. Password parameters require passwords to have a minimum password length of 8 characters and a maximum password history of 60 days. Passwords must include lowercase and uppercase alphabetic characters, a numbers, and a special character. Authentication to the vCenter application for managing the hypervisors rely on the Active Directory credentials and authentication process via lightweight directory access protocol (LDAP). Access to infrastructure management components is restricted to authorized user access roles and functions. The Company restricts system and security administrative access solely to system, network and security administrators that require such access to perform job responsibilities.

User access is provisioned to employees based on approved levels of access requested by direct managers and HR. Workflow tickets are generated and assigned to administrators of respective business applications and folders for provisioning access. The HR team initiates access termination requests upon termination of employees. User access to business systems and applications is removed upon notification by administrators for each system and the completion of the access revocation process is tracked and documented within the workflow ticketing system.

Remote access onto all PhoenixNAP environments by employees is permitted only through encrypted virtual private network (VPN) connections. Dual factor authentication is required for access to VPN access.

Client users access the PhoenixNAP portal to manage and monitor their public or private cloud instances. An initial administrator account for PhoenixNAP portal access is provisioned to external users during the client onboarding process. All additional users are provisioned and revoked by client administrator users.

Physical Security

The following description of physical security relates solely to PhoenixNAP's Phoenix data center and excluded colocated facilities.

Physical access to the Phoenix data center facility and office facility is restricted by electronic badge access doors and monitored by security cameras. The facility is staffed by security guards at all times to monitor access to the building. Visitor access to the data center is restricted to registered visitors. All visitors must wear a visitor's badge and be escorted by PhoenixNAP employees at all times.

Physical access to sensitive areas of the data center where server stacks and internet connections are located are restricted to authorized personnel by three-factor authentication. Users must present an electronic badge, perform a retinal scan, and input an electronic pin for access. Anti-tailgate sensing mechanisms are in place to prevent individuals from tailgating to sensitive areas of the data center. Security guards are notified when tailgating attempts are detected.

Physical access to the data center and corporate office facility is provisioned to employees upon authorization from the human resources team. Physical access is revoked by the facilities team upon notification from the human resources team of a termination. The access provisioning and revocation process is documented and tracked within the workflow ticketing system.

Long-term physical access to the data center may be provided to clients and users of PhoenixNAP's colocation services. Access to the data center facility is provisioned upon receipt of a Facility Access Application form from an authorized client contact. Physical access to the data center for external users is removed upon customer request. A badge administrator will notify the critical infrastructures team to disable access and change cage combinations within 24 hours. The critical infrastructures team is the team responsible for managing and monitoring operations of the data center.

Environmental Security

The following description of environmental security relates solely to PhoenixNAP's Phoenix data center and excluded colocated facilities.

Environmental and operation conditions of PhoenixNAP's Phoenix data center is monitored at all times by members of the critical infrastructures team. The Critical Environment Department monitors the temperature, humidity, power levels, and UPS performance for the data center. Alerts are generated and sent to members of the Critical Environment Department when configured thresholds are reached. Environmental protection controls and monitoring systems include the following:

- Redundant cooling systems with water chillers
- Redundant natural gas generators
- Redundant battery failovers
- Redundant Internet connectivity and communication lines.
- Smoke detectors
- Temperature sensors
- Humidity sensors
- Fire suppression systems

Environmental protection monitoring devices and controls receive maintenance at least annually. As part of the maintenance process, all systems are tested.

Monitoring

Logging and monitoring software has been implemented to monitor and evaluate ongoing system performance and resource utilization needs. Notifications are sent to the cloud infrastructure team when predefined thresholds have been reached to allow for escalations and corrective actions to take place. Virtual machines are migrated to backup hosts to optimize performance when issues or resource limitations arise. Security events from firewalls and logical access monitoring devices are routed to a logging software which is reviewed and monitored by members of the information security team. Alerts are sent for critical events when event thresholds have been met. Vulnerability scans are performed on a monthly basis. Management identifies corrective actions for risks and threats identified during periodic scans.

Change Management

Policies and procedures for assessment, authorization, testing, and approval of changes are documented in PhoenixNAP's change management policy. As part of the change management process, a Change Advisory Board has been created which includes broad representation from the Company. The listing of changes is reviewed on a weekly basis for appropriateness and status monitoring.

Changes are segregated between infrastructure and development changes. Software development changes are applicable to the PhoenixNAP portal that is accessed by clients. Changes are evaluated as part of the change management process for communication requirements to external and internal members. Email communications are sent to parties that require communications as results of changes to system and user responsibilities or design. System changes are evaluated for risk as part of the request process. All non-minor changes must be approved by broad representation of the Company, including approval by the Information Security Team, the Infrastructure Team, and the Change Management Team prior to implementation. System changes are reviewed post implementation by the Change Management Team to ensure all change processes had been followed and completed as requested. Though minor changes do not require approval from different team members, notifications are sent to each team in order to notify and identify the changes that will take place. Separate environments are used for development, testing, and production. The ability to migrate changes into the production environment is restricted to authorized personnel.

Backup and Disaster Recovery

Backup policies and procedures have been implemented to backup information at the PhoenixNAP corporate environment as well as the management infrastructure of the cloud environment. Backups are performed on a daily basis and information is replicated across multiple storage arrays. Members of the Cloud Infrastructure Team are notified if backup processes fail to complete successfully. Backups for client information and storage arrays are performed as an additional service that is provided to users of PhoenixNAP's Disaster Recovery and Backup services.

PhoenixNAP management has developed business continuity plans for business resumption processes and procedures in the event of service disruptions.

Incident Management

PhoenixNAP management has established robust policies and procedures for handling and responding to incidents that have been identified from internal control detection processes and external notifications. Incident handling policies procedures are documented within the Company's Incident Response Plan (IRP). Operations and security personnel perform investigation and corrective actions for incidents that have been escalated by internal or external users. Incidents and issues are tracked within the Company's ticketing and task assignment system.

H. COMPLEMENTARY USER ENTITY CONTROLS

PhoenixNAP's Cloud Services Information Technology General Controls and the controls over the Cloud Services Information Technology General Controls were designed with the assumption that certain controls would be placed in operation by user entities. This section describes the controls that are necessary to be in effective operation at user entities to achieve certain control objectives at PhoenixNAP. User entities should determine whether they have established controls to provide reasonable assurance that:

- Incidents and complaints are escalated and communicated to the PhoenixNAP team for investigation. (Control objective 1 – Information Security Policies and Procedures)
- Credentials and passwords for accessing PhoenixNAP systems are maintained, protected, and restricted to authorized parties. (Control objective 2 – Logical Access)
- Access to the PhoenixNAP portal and cloud environment is restricted to authorized personnel. (Control objective 3 – Physical Security)
- Employees with physical access to PhoenixNAP data centers are authorized and instances for access removals are communicated to PhoenixNAP in a timely manner. (Control objective 3 – Physical Security)
- Firewalls and other logical access controls are monitored and managed by user entity personnel. (Control objective 4 – Systems Security and Monitoring)
- Requests and changes to system parameters are authorized, testing, and approved by user entities management. (Control objective 5 – Systems Development and Change Management)

Section IV: Independent Service Auditor's Description of Tests of Controls and Results

This section presents the following information provided by PhoenixNAP:

- The control objectives specified by the management of PhoenixNAP
- The controls established and specified by PhoenixNAP to achieve the specified control objectives

Also included in this section is the following information provided by the service auditor:

- A description of the tests performed by the service auditor to determine whether the service organization's controls were operating with sufficient effectiveness to achieve specified control objectives. The service auditor determined the nature, timing, and extent of the testing performed.
- The results of the service auditor's tests of controls.

The service auditor performed observation and inspection procedures as they relate to system-generated reports, queries, and listings to assess the accuracy and completeness of the information used in the service auditor's tests of controls.

1. Information Security Policies and Procedures

Control Objective: Controls provide reasonable assurance that information security policies and procedures have been developed and are communicated to users of the system.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Personnel are required to read and acknowledge policies over ethical conduct, protection of information security, and statements of confidentiality and privacy practices at time of hire.	**A.** Inspected policy acknowledgments for a sample of employees to determine whether employees are required to acknowledge policies at the time of hire.	**A. Deviations noted.** Company policies were not acknowledged by 2 of 15 new hires selected for testing.
2. Incident handling policies and procedures are documented within the Company's Incident Response Plan (IRP).	**A.** Inspected the Incident Response Policy (IRP) to determine whether policies and procedures exist for evaluating and responding to events.	**A.** No deviations noted.
3. Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints are published and available on the intranet.	**A.** Observed the intranet operation to determine whether policies and procedural documents for processes such as reporting of operational failures, incidents, system problems and concerns are made available to internal users.	**A.** No deviations noted.
4. During the annual risk assessment and management process, personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.	**A.** Inspected the risk assessment to determine whether a risk assessment is performed and updated on an annual basis.	**A.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
5. The entity has appointed an Information Security Officer (ISO) who is responsible and accountable for the design, operation and monitoring of the Company's security and control environment.	**A.** Inspected the appointment of the role and job description for the ISO to determine whether the responsibility and accountability for the design, operation and monitoring of the Company's security and control environment has been appointed to the ISO.	**A.** No deviations noted.
6. A description of the Cloud Services Information Technology General Controls System and services provided by PhoenixNAP is made available to external users of the systems on the customer-facing website.	**A.** Inspected the customer facing website to determine whether a description of the system and services is made available to external users.	**A.** No deviations noted.
7. Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are communicated to clients during the client account creation process.	**A.** Observed the new account setup process operation to determine whether the MSA and SLA are required to be acknowledged during the new account setup process.	**A.** No deviations noted.
	B. Inspected the MSA and SLA to determine whether customer responsibilities for reporting incidents and the process for reporting incidents are included in the MSA and SLA.	**B.** No deviations noted.

2. Logical Security

Control Objective: Controls provide reasonable assurance that logical access to the network, applications and data is restricted to authorized personnel.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Unique user IDs and passwords are required to access the cloud network infrastructure and management infrastructure environment. Password parameters include: • Password length minimum: 8 characters • Password forced expiration: 60 days • Password forced complexity: enabled	**A.** Inspected user access listings for all production platforms to determine whether unique user IDs are required.	**A.** No deviations noted.
	B. Inspected password parameters to determine whether password parameters are configured as described in the control activity.	**B.** No deviations noted.
2. User access is provisioned to employees based on the approved levels of access requested by direct managers and HR. Workflow tickets are generated and assigned to administrators of respective business applications and folders for provisioning access.	**A.** Inspected user access requests for a sample of new hires to determine whether access was authorized.	**A.** No deviations noted.
3. The HR team initiates access termination requests upon termination of employees. User access to business systems and applications is removed upon notification by administrators for each system and the completion of the access revocation process is tracked and documented within the workflow ticketing system.	**A.** Inspected user access revocation requests for a sample of terminated employees to determine whether access is revoked upon termination.	**A.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
4. PhoenixNAP restricts system and security administrative access to only system, network and security administrators that require such access to perform job responsibilities.	**A.** Inspected system access listings for administrative access account users to determine whether administrative access is restricted to authorized individuals based on job responsibilities.	**A.** No deviations noted.
5. Access to infrastructure management components is restricted to authorized user access roles and functions.	**A.** Inspected the listing of user roles available to be created to determine whether role based access is used for limiting access.	**A.** No deviations noted.
6. An initial administrator account for PhoenixNAP portal access is provisioned to external users during the client onboarding process. All additional users are provisioned and revoked by external admin users.	**A.** Observed the new account setup process operation to determine whether clients are responsible for creating external user accounts.	**A.** No deviations noted.
7. Local administrator rights on systems have been restricted to authorized personnel to limit the ability to install software.	**A.** Inspected system settings to determine whether the ability to install software on workstations and laptops is restricted to IT support personnel.	**A.** No deviations noted.
8. Access to the Management Infrastructure of the Cloud Environment requires access through a bastion host. dual factor authentication is required for access to the bastion host.	**A.** Observed a user access the cloud infrastructure to determine whether access connectivity required connecting through a bastion host and to determine whether dual factor authentication was required.	**A.** No deviations noted.

3. Physical Security

Control Objective: Controls provide reasonable assurance that physical access to systems equipment and data is restricted to authorized personnel.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Physical access to the Phoenix data center facility and office facility is restricted by electronic badge access doors and monitored by security cameras.	**A.** Observed the PhoenixNAP data center in operation to determine whether physical access requires an electronic badge for access.	**A.** No deviations noted.
	B. Observed the PhoenixNAP data center entrance operation to determine whether security cameras exist to monitor entranceways.	**B.** No deviations noted.
	C. Observed the PhoenixNAP corporate office facility in operation to determine whether physical access requires an electronic badge for access.	**C.** No deviations noted.
	D. Observed the PhoenixNAP corporate office facility in operation to determine whether security cameras exist to monitor entrance ways.	**D.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
2. Physical access to sensitive areas of the Phoenix data center where server stacks and internet connections are located are restricted to authorized personnel by three factor authentication. Users must present an electronic badge, perform a retinal scan, and input an electronic pin for access.	**A.** Observed an authorized individual access the server area of the data center facility to determine whether three factor authentication was required for access.	**A.** No deviations noted.
3. Anti-tailgate sensing mechanisms are in place to prevent individuals from tailgating to sensitive areas of the Phoenix data center. Security guards are notified when tailgating attempts are detected.	**A.** Observed an individual attempt to tailgate to a sensitive area of the data center to determine whether anti-tailgate sensing mechanisms alert the security team when a tailgate attempt is detected.	**A.** No deviations noted.
4. Physical access to the Phoenix data center and corporate office facility is provisioned to employees upon authorization from the human resources team. Physical access is revoked by the facilities team upon notification from the human resources team of a termination. The access provisioning and revocation process is documented and tracked within the workflow ticketing system.	**A.** Inspected physical access authorization forms for a sample of new hire employees to determine whether access was authorized by the HR team.	**A.** No deviations noted.
	B. Inspected access removal request forms for a sample of terminated employees to determine physical access is revoked by the facilities team upon notification from the human resources team of a termination.	**B.** No deviations noted.

Controls Specified by PhoenixNAP		Testing Performed by Service Auditors	Results of Tests
		C. Inspected physical access listings to determine whether physical access for terminated employees had been revoked.	**C.** No deviations noted.
5.	Access to the Phoenix data center facility is provisioned upon receipt of a Facility Access Application form from an authorized client contact.	**A.** Inspected Facility Access Application Forms for a sample of new external user access accounts to determine whether access is provisioned upon receipt of a Facility Access Application form from an authorized client contact.	**A.** No deviations noted.
6.	Physical access to the Phoenix data center for external users is removed upon customer request.. A badge admin will notify the critical infrastructures team to disable access and change cage combinations within 24 hours.	**A.** Inspected a sample of physical access revocation requests and badge access logs to determine whether physical access is removed timely upon customer request.	**A.** No deviations noted.
7.	Visitor access to the Phoenix data center is restricted to registered visitors. All visitors must wear a visitor's badge and be escorted by PhoenixNAP employees at all times.	**A.** Observed the PhoenixNAP data center operation to determine whether visitors are required to wear a visitor badge and be escorted by a PhoenixNAP employee during the visit.	**A.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
8. Attestations and reports on control environments for third party data centers are reviewed on an annual basis by the security team.	**B.** Inspected the SOC reports obtained by the ISO for third party data centers to determine whether the reports had been obtained and reviewed by the ISO.	**B.** No deviations noted.

4. Systems Security and Monitoring

Control Objective: Controls provide reasonable assurance that systems and security components are monitored and maintained.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Firewalls are in place to monitor and block unauthorized internet facing traffic to each environment.	**A.** Inspected the firewall monitoring system to determine whether network traffic is monitored and unauthorized network traffic is blocked.	**A.** No deviations noted.
2. Connectivity to the PhoenixNAP portal is encrypted.	**A.** Inspected the PhoenixNAP portal to determine whether HTTPS encryption is used on the portal provided for external users to manage their virtual environment.	**A.** No deviations noted.
3. Remote access onto the PhoenixNAP environment by employees is permitted only through encrypted virtual private network (VPN) connections. Dual factor authentication is required for access to VPN access.	**A.** Inspected remote access configurations to determine whether encryption is in place for the agent connection.	**A.** No deviations noted.
	B. Observed a user access the internal network through the agentless portal to determine whether HTTPS connection is in place.	**B.** No deviations noted.
	C. Inspected VPN client system settings to determine whether two factor authentication is required for external access.	**C.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
4. Security events from firewalls and logical access monitoring devices are routed to a logging software which is reviewed and monitored by members of the information security team. Alerts are sent for critical events when event thresholds have been met.	**A.** Inspected network event monitoring system configurations to determine whether system security is monitored and alerts are sent for critical events when event thresholds have been met.	**A.** No deviations noted.
5. Antivirus software is installed on workstations, laptops, and servers. Scheduled scans take place on a weekly basis and members of the Information Security Team are notified when malware and threats are detected.	**A.** Inspected the antivirus management system console to determine whether servers and workstations were managed and monitored by antivirus software.	**A.** No deviations noted.
	B. Inspected antivirus configurations to determine whether scheduled scans take place on a weekly basis.	**B.** No deviations noted.
	C. Inspected antivirus notification configurations to determine whether members of the Information Security Team are notified when malware and threats are detected.	**C.** No deviations noted.
6. Antivirus software is configured to receive an updated virus signature at least daily. The Network Operations Team receives a report of devices that have not been updated in 30 days and follows up on the devices.	**A.** Inspected antivirus system settings to determine whether antivirus software is configured to receive updates daily.	**A.** No deviations noted.

Controls Specified by PhoenixNAP		Testing Performed by Service Auditors	Results of Tests
		B. Inspected antivirus system settings to determine whether the system is configured to notify the Network Operations Team when antivirus has not been updated on devices in 30 days.	**B.** No deviations noted.
7.	Updates and patches for PhoenixNAP systems are applied on a quarterly basis.	**A.** Inspected patch application logs for a sample of quarters to determine whether patches to machines are applied on a quarterly basis.	**A.** No deviations noted.
8.	Vulnerability scans are performed monthly. Management identifies corrective actions for risks and threats identified during periodic scans.	**A.** Inspected vulnerability scan reports for a sample of months to determine whether vulnerability scans are performed on a monthly basis and corrective actions are taken based on the results of scanning.	**A.** No deviations noted.
9.	Operations and security personnel perform investigation and corrective actions for incidents that have been escalated by internal or external users.	**A.** Inspected incident tickets for a sample of incidents to determine whether incidents are investigated and corrective actions are performed.	**A.** No deviations noted.

5. Systems Development and Change Management

Control Objective: Controls provide reasonable assurance that system changes are authorized, tested, and approved.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Policies and procedures for assessment, authorization, testing, and approval of changes are documented in the change management policy.	**A.** Inspected the change management policy to determine whether policies and procedures for change processes are documented.	**A.** No deviations noted.
2. System changes are evaluated for risk as part of the request process. All non-minor changes must be approved by broad representation of the Company, including approval by the Information Security Team, the Infrastructure Team, and the Change Management Team prior to implementation.	**A.** Inspected change tickets to determine whether changes are evaluated for risk as part of the approval process.	**A.** No deviations noted.
	B. Inspected change tickets for a sample of changes to determine whether non minor changes had been reviewed and approved by members of the Information Security Team, Infrastructure Team, and Change Management Team prior to implementation.	**B.** No deviations noted.
3. System changes are reviewed post implementation by the Change Management Team to ensure all change processes had been followed and completed as requested.	**A.** Inspected change tickets for a sample of changes to determine whether system changes were reviewed and approved post implementation by a Change Management Team member.	**A.** Deviation noted. The review and approval was not performed for 1 of 15 changes selected for testing.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
4. Separate environments are used for development, testing, and production.	**A.** Inspected configurations for the development, testing, and production environment to determine whether separate environments are used.	**A.** No deviations noted.
5. The ability to migrate changes into the production environment is restricted to authorized personnel.	**A.** Inspected listing of individuals with access to migrate changes to the production environment to determine whether access was restricted to authorized personnel.	**A.** No deviations noted.

6. Environmental

Control Objective: Controls provide reasonable assurance that backups are performed and environmental protections are installed to support the availability of systems and the recoverability of data.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
1. Backups for data storage and management infrastructure are performed on a daily basis. Members of the Cloud Infrastructure Team are notified if backup processes fail to complete successfully.	**A.** Inspected backup system configurations to determine whether backups for the cloud environment are performed on a daily basis.	**A.** No deviations noted.
	B. Inspected backup system configurations to determine whether members of the Cloud Infrastructure Team are notified of backup job failures.	**B.** No deviations noted.
2. Logging and monitoring software has been implemented to monitor and evaluate ongoing system performance and resource utilization needs. Notifications are sent to the cloud infrastructure team when predefined thresholds have been reached.	**A.** Observed the monitoring software operation to determine whether logging and monitoring software is used to monitor and evaluate ongoing system performance and resource utilization needs.	**A.** No deviations noted.
	B. Inspected the monitoring software system settings to determine whether the software is configured to generate automatic alerts when predefined thresholds are met.	**B.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
	C. Inspected the monitoring software system settings to determine whether the software is configured to create tickets automatically when predefined thresholds are met.	**C.** No deviations noted.
3. Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers Redundant environmental protection controls are in place for each of the environmental control systems listed.	**A.** Observed the data center facility in operation to determine whether the following environmental controls were in place: • Cooling systems • Uninterruptible power supply (UPS) • Natural gas generators • Smoke detectors • Temperature sensors • Humidity sensors • Fire suppression systems	**A.** No deviations noted.
	B. Observed the data enter facility operation to determine whether redundant environmental controls are in place.	**B.** No deviations noted.

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
4. The Critical Environment Department monitors the temperature, humidity, power levels, and UPS performance for the data center. Alerts are generated and sent to members of the Critical Environment Department when configured thresholds are reached.	**A.** Inspected environmental monitoring system configurations to determine whether members of the Critical Environment Department are notified when environmental controls thresholds are met.	**A.** No deviations noted.
5. Environmental protections receive maintenance at least annually. As part of the maintenance process, environmental protection controls are tested.	**A.** Inspected maintenance records for environmental protection systems to determine whether maintenance is performed at least annually.	**A.** No deviations noted.
	B. Inspected results of environmental protections testing to determine whether environmental protections systems are tested during maintenance.	**B.** No deviations noted.
6. Business continuity plans have been developed and documented.	**A.** Inspected business continuity plans to determine whether business continuity plans have been developed and documented.	**A.** No deviations noted.

7. Subservice Organization Monitoring

Control Objective: Controls provide reasonable assurance that the performance of subservice organizations monitored and controls related to security are evaluated.

Description of Controls

Controls Specified by PhoenixNAP	Testing Performed by Service Auditors	Results of Tests
7. Attestations and reports on control environments for third party data centers are reviewed on an annual basis by the security team.	**C.** Inspected the SOC reports obtained by the ISO for third party data centers to determine whether the reports had been obtained and reviewed by the ISO.	**C.** No deviations noted.

For more information regarding the report, contact:

Steven Freeman | Director of Information Security
PhoenixNAP, LLC
stevef@cwie.net

For more information on Plante Moran, contact:
Timothy R. Bowling, CPA, CCSK | Partner
Plante Moran
312-980-2927
tim.bowling@plantemoran.com

plantemoran.com