PEAK 10, INC.

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT FOR THE DATA CENTER OPERATIONS AND CLOUD SERVICES SYSTEM

FOR THE PERIOD OF NOVEMBER 1, 2016, TO OCTOBER 31, 2017

Attestation and Compliance Services

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Management of Peak 10, Inc.:

We have examined management's assertion that during the period November 1, 2016, to October 31, 2017, Peak 10, Inc. ("Peak 10") maintained effective controls over the Data Center Operations and Cloud Services system (the "system"), for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements; and
- the system was available for operation and use to meet the entity's commitments and system requirements.

As indicated in the description, Peak 10 uses BAE Systems, Inc. ("BAE Systems") for threat detection, log file monitoring and security scanning services. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at BAE Systems are suitably designed and operating effectively. The description presents Peak 10's system; its controls relevant to the applicable trust services criteria; and the types of controls that Peak 10 expects to be implemented, suitably designed, and operating effectively at the BAE Systems to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at BAE Systems. Our examination did not extend to the services provided by BAE Systems, and we have not evaluated whether the controls management expects to be implemented at BAE Systems have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2016, to October 31, 2017.

Peak 10's management is responsible for the attached assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the Data Center Operations and Cloud Services system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Peak 10's relevant controls over the security and availability of the Data Center Operations and Cloud Services system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, Peak 10's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CPA Canada applicable trust services criteria.

Schellman & Company, LLC

Tampa, Florida
November 17, 2017

MANAGEMENT'S ASSERTION

November 17,2017

During the period November 1, 2016, through October 31, 2017, Peak 10, Inc. ("Peak 10") maintained effective controls over the Data Center Operations and Cloud Services system (the "system"), for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements; and
- the system was available for operation and use to meet the entity's commitments and system requirements.

The attached system description identifies the aspects of the Data Center Operations and Cloud Services system covered by the assertion.

David Kidd
Vice President of Governance, Risk and Compliance

SYSTEM DESCRIPTION OF THE DATA CENTER OPERATIONS AND CLOUD SERVICES SYSTEM

Company Background

Peak 10, Inc. ("Peak 10") is a data center operator providing hybrid information technology (IT) infrastructure solutions spanning colocation, interconnection, cloud, managed solutions and professional services. The company combines its data centers and portfolio of hybrid IT services with localized engineering and support to serve companies nationwide. The Peak 10 management team is comprised of customer-focused professionals.

Description of Services Provided

Products and Services Overview

Peak 10 delivers scalable, reliable and secure IT infrastructure solutions that include data center, network, and cloud services. These services help maximize user entities' existing technology investments to better meet their current and future technology needs. From managed colocation to burstable bandwidth and cloud computing, Peak 10 IT infrastructure solutions are designed to easily scale and adapt to user entities' changing business needs.

Data Center Services

Data center services, including colocation and cloud services, are available through Peak 10's network of strategically located, secure data centers. Comprised of facilities, network, power and critical infrastructure; the Peak 10 data center services allow user entities to utilize existing investment in computing equipment and networking gear or leverage Peak 10's cloud environment.

Data Center Details

Peak 10 currently operates multiple data center facilities in 10 markets in the United States and serves companies domestically and internationally. Each of the Peak 10 data centers adheres to structured processes and procedures that ensure user entities technology assets are available and secure.

Technology and Expertise

Peak 10 facilities are staffed by a general manager and director of service delivery. The data center facilities are also manned by on-site technical experts 24/7/365 to help ensure equipment and/or critical applications are up and running, immediately accessible and secure. In addition, Peak 10 employs a comprehensive training program to help ensure that Peak 10 data center personnel are trained data center operations and security.

Technology and Security

Peak 10 data center facilities incorporate multiple physical and operational security features and protocols including the following:

- Biometric fingerprint readers
- Card/Personal Identification Number (PIN) access
- Combination lock cabinets
- 24/7/365 monitored video surveillance with video stored for review for non-repudiation.
- Multifactor authentication system
- Staff trained to maintain stringent physical security policies and controls
- Perimeter doors alarmed and monitored
- Exterior landscaping to prevent concealment of intruders

Environmental Controls/Redundancy

Designed for efficiency and cost savings, Peak 10 data centers incorporate efficient cooling solutions to ensure consistent temperature and humidity levels for protection of mission-critical technology. The data centers are also equipped with distributed cooling with cold aisle containment to help reduce energy costs. In addition, critical facility components (e.g., generators, uninterruptible power supply (UPS) and cooling systems) throughout Peak 10 data centers are redundant. With this level of redundancy, Peak 10 can perform regular preventative maintenance on the equipment with no impact to user entities.

Network

The Peak 10 network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. It incorporates redundancy to ensure reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center. Peak 10 data centers are equipped with network features, including:

- Dual path
- Redundant carrier class infrastructure
- 10/100/1000Mb ports available
- Redundant Internet access in 100Mb/1Gb/10Gb
- Multiple diverse, ring-protected fiber providers
- Multiple, redundant Tier 1 Internet access providers
- Carrier-neutral telecom services
- Metro Ethernet at 10 Mbps, 100 Mbps, 1 Gbps

<u>Peak 10 Network Services</u>

Peak 10 offers network services to facilitate the communication of user entity workloads running in Peak 10 data centers or the cloud with dependent systems and their users. Primary services include Internet access, Virtual Private Line (VPL) service and Ethernet Private Line (EPL) service. All options can be tailored to user entities' specific needs and are backed by 24/7/365 technical support.

Consisting of a multi-carrier, redundant architecture, the Peak 10 network has no single point-of-failure. Connectivity at each data center consists of a minimum of two fiber providers with dual entry points providing multiple gigabits of bandwidth capacity. All sites have multiple high quality Internet providers and are inter-connected via a private, meshed network. This configuration ensures network accessibility of business critical applications residing in Peak 10 data centers and/or in the Peak 10 cloud.

Peak 10 has standardized on Cisco Systems as a service provider for network architecture Cisco's ASR9000 platform provides core routing functionality in each market. The distribution layer is powered by Cisco Nexus 7000 and Catalyst 6500 series switches.

Peak 10 provides one or more local area network (LAN) connections to users' cabinets or cage space. Where redundant Peak 10 connections are needed to connect to user entities' redundant access devices, they are delivered from separate access layer switches for the final connectivity component involved in access to the Internet or other Peak 10 facilities.

Peak 10 Network Features

- Redundant paths for Internet connectivity providing connectivity to other Peak 10 locations
- Redundant carriers per location, providing flexibility to users when choosing private connectivity to their premises and trusted third parties
- Dynamic, performance optimized routing via automated, ongoing hop-count and latency monitoring Burstable services to accommodate unforeseen or seasonal demand
- Redundant, carrier-class infrastructure with no single points of failure

- 300 Gb/s aggregate intersite network capacity
- 230 Gb/s aggregate Internet capacity
- Choice of 10, 100, 1000, or 10000 Mbps access port options

Internet Access

Peak 10 Internet access solutions provide the flexibility and scalability necessary to manage expanding communications and data requirements. These services leverage industry-leading technology to optimize traffic routing to external networks to ensure availability and performance over the Internet.

In addition to bandwidth, value-add and add-on services are available for utilization monitoring, domain name service (DNS) management and IP failover services.

Features include:

- Multiple physical connectivity options including 100 Mbps, 1 Gbps and 10 Gbps network ports in addition to cloud connectivity
- Rapid installation, implementation and service change turnaround times
- Carrier neutrality for private networking needs used to connect Peak 10 housed resources to other corporate resources and third parties
- Comprehensive, web-based portal for bandwidth usage reporting
- Burstable and fixed limit subscription options
- Add-on managed security services, including firewall, virtual private network (VPN), and intrusion detection systems
- Traffic traverses Peak 10's private network without affecting Internet bandwidth usage
- Multiple 10 Gbps private connections between Peak 10 facilities

Private Network Services

User entities can use multiple Peak 10 locations to geographically diversify portions of their IT infrastructure. Connectivity between these locations is used to replicate data for a production and disaster recovery use case or to synchronize data in the case of a multi-site, active/active application deployment. Peak 10's private network provides a secure and scalable alternative to sending the data through a public Internet connection or subscribing to a private, inflexible carrier solution. Private network services can be used to carry data, video and voice services together over the same connection. Services do not traverse the public Internet and are not shared services, providing both security and reliability.

Virtual Private LAN Service

Virtual Private LAN is Peak 10's private, routed network service. It connects distinct IP subnets at each location and can provide routing to remote subnets as well for those topologies with multiple wide area network (WAN) connections. Virtual Private LAN removes the capital requirements of purchasing routing devices and the operational requirement of managing dedicated equipment.

Virtual Private LAN-specific features:

- Independent, virtual private router interfaces to provide isolated traffic flows for IP services
- Eliminate the need for user-provided routers or firewalls for IP segmentation and routing
- Lower bandwidth usage due to routed segmentation and limitation of broadcast traffic
- Scalable and available as a burstable or fixed bandwidth subscription
- Redundant access layer connectivity options are available

EPL Service

EPL provides user entities with the ability to extend local network segments, commonly referred to as a Layer 2 connectivity based on the Open Systems Interconnection (OSI) model. The service can be implemented as a scalable point-to-point or a point-to-multipoint topology. EPL is available in a wide range of bandwidth speeds and is ideal for running services and applications that require local network to be presented across geographically disparate environments within Peak 10 data centers. Additionally, user entities may choose to use this service as a component of their disaster recovery design where it is desirable not to modify local IP addresses during the failover process. EPL services also enable burstable workload scenarios where applications can be moved between locations or clouds without changes to the network configuration.

EPL-specific features:

- Independent virtual local area network (VLAN) segmentation for security
- No routing or firewall hardware required
- Utilize layer 2 switched networking to communicate across the network instead of layer 3 Transmission Control Protocol (TCP)/IP address
- Allow devices at each location to communicate as if local to each other while being on the same IP subnet
- Eliminate the use of additional routing devices to help lower latency

Data Services

Backup and Restore

Peak 10 will backup user entities' data on Peak 10 hardware, manage data backup on user entities' provided hardware, rotate tapes and manage user entities' backup library or replicate data to alternate sites.

Tape Rotation

- Peak 10 will eject media and insert next media in sequence defined by the user entities
- User entities' owned backup device and storage in the user entities' cage(s)
- Rotation scheduled by user entities

Electronic Vaulting Services

- User entity-identified data backed up to geographically remote data center
- Data sent over a secure connection
- Automated backups

Storage Services

- Enhanced tools for online management
- Security and availability
- Real-time monitoring

Availability Monitoring

- Suitable for monitoring application-specific network ports, web content and e-mail availability
- Includes up/down monitoring, TCP/User Datagram Protocol (UDP) port monitoring, Hypertext Transfer Protocol (HTTP)/ Hypertext Transfer Protocol Secure (HTTPs) content verification and e-mail round-trip monitoring
- Alerts automatically delivered via text message or e-mail to designated contact(s)

Basic Up/Down Monitoring

- Up/Down ICMP (ping) monitoring
- Suitable for any device with an IP address
- Alerts are automatically delivered via text message or e-mail to designated contact(s)

Performance Monitoring

- Suitable for most network devices which utilize the Simple Network Management Protocol (SNMP) to report performance metrics
- The subscription trends and alerts based on up/down, web and e-mail application availability, central processing unit (CPU) utilization, file system utilization, physical and virtual memory utilization, service and process status, and network interface usage, errors and discards
- Alerts are automatically delivered to the designated contact(s)

Cloud Services

The Peak 10 Cloud delivers a comprehensive computing model that allows user entities to grow their IT infrastructure as their business demands without sacrificing security, reliability or performance.

The Peak 10 Cloud enables on-demand network access to a multi-tenant environment of logically segmented pools of configurable computing resources that can be rapidly provisioned. Using the Infrastructure as a Service (IaaS) model, the Peak 10 Cloud provides on-demand resources via the Internet and/or private network connections.

The Peak 10 Cloud allows user entities to subscribe to the infrastructure and platform assets that their businesses need, while maintaining scalable, reliable and secure technology. As a result, they can operate, maintain and improve operations, enhance technology planning and manage capital/operational finances.

Enterprise Cloud

The Peak 10 Enterprise Cloud delivers compute infrastructure from scalable, enterprise-class, multi-tenant clusters. The clusters go through a commissioning process to verify that no single point of failure exists. Peak 10's Enterprise Cloud can be utilized as a standalone compute environment or can be logically connected to physical or other cloud environments.

Private Cloud

Peak 10's Private Cloud offers scale and flexibility in both virtual and dedicated service delivery models. If compliancy or user entities demands require dedicated resources or completely dedicated equipment, the Peak 10 Private Cloud can be configured to deliver the kind of platform that is needed. Peak 10 Private Cloud resource pools combine logical security and best practices with the flexibility and cost efficiency of multi-tenancy.

Recovery Cloud

The Peak 10 Recovery Cloud provides a highly flexible disaster recovery (DR) solution that ensures rapid recovery of mission-critical applications and data. Recovery Cloud enables user entities to take advantage of the reduced costs associated with multi-tenancy while accessing the necessary cloud resources to restore services in the event of a site failure quickly, securely and regardless of where their production environment is housed. It features continuous data protection (CDP) style replication to ensure data and applications are backed up in near real-time.

Infrastructure and Software

The Peak 10 in-scope infrastructure consists of multiple network devices, operating system platforms and supporting software tools, as shown in the table below:

Primary Infrastructure			
Name	**Description**	**Operating System/Platform**	**Physical Location**
Badge Card Access System (EntraPass)	The badge card access system is utilized in conjunction with the biometric recognition access system to control access to the greater data center facilities and the raised-floor within the data center facilities.	Kantech	All data centers
Biometric Recognition Access System (EntraPass)	The biometric recognition access system is utilized in conjunction with the badge card access system to control access to the greater data center facilities and the raised-floor within the data center facilities.	Kantech	All data centers
Firewalls	Corporate firewalls are utilized to restrict traffic into the management network, and service delivery firewalls are utilized to filter and route traffic for customer-specific environments.	Fortigate FortiOS	All data centers
Management Services Backup Servers** (Simpana)	Automated backup system software and network of servers that provide backup and recovery for subscribing customers.	CommVault	All data centers
Routers and Switches	Routers and switches are utilized to route network traffic.	Cisco NXOS	All data centers
Virtual Hypervisor	VMware vCenter server that provides authentication and restricts access to customer virtual environments.	VMware vCenter (Windows Server 2012, R2)	Charlotte, Atlanta, Nashville and Louisville
VMware Hosts	VMware ESX hosts for running client virtual machines.	VMware (ESXi 6.0)	Charlotte, Atlanta, Nashville and Louisville
Web Portal	Customer portal system, through which customers manage their virtual machines.	Embotics vCommander	Charlotte, Atlanta, Nashville and Louisville

*** Backup services are provided to subscribing customers only.*

People

Peak 10 utilizes the following functional areas of operations to support the Data Center Operations and Cloud Services system:

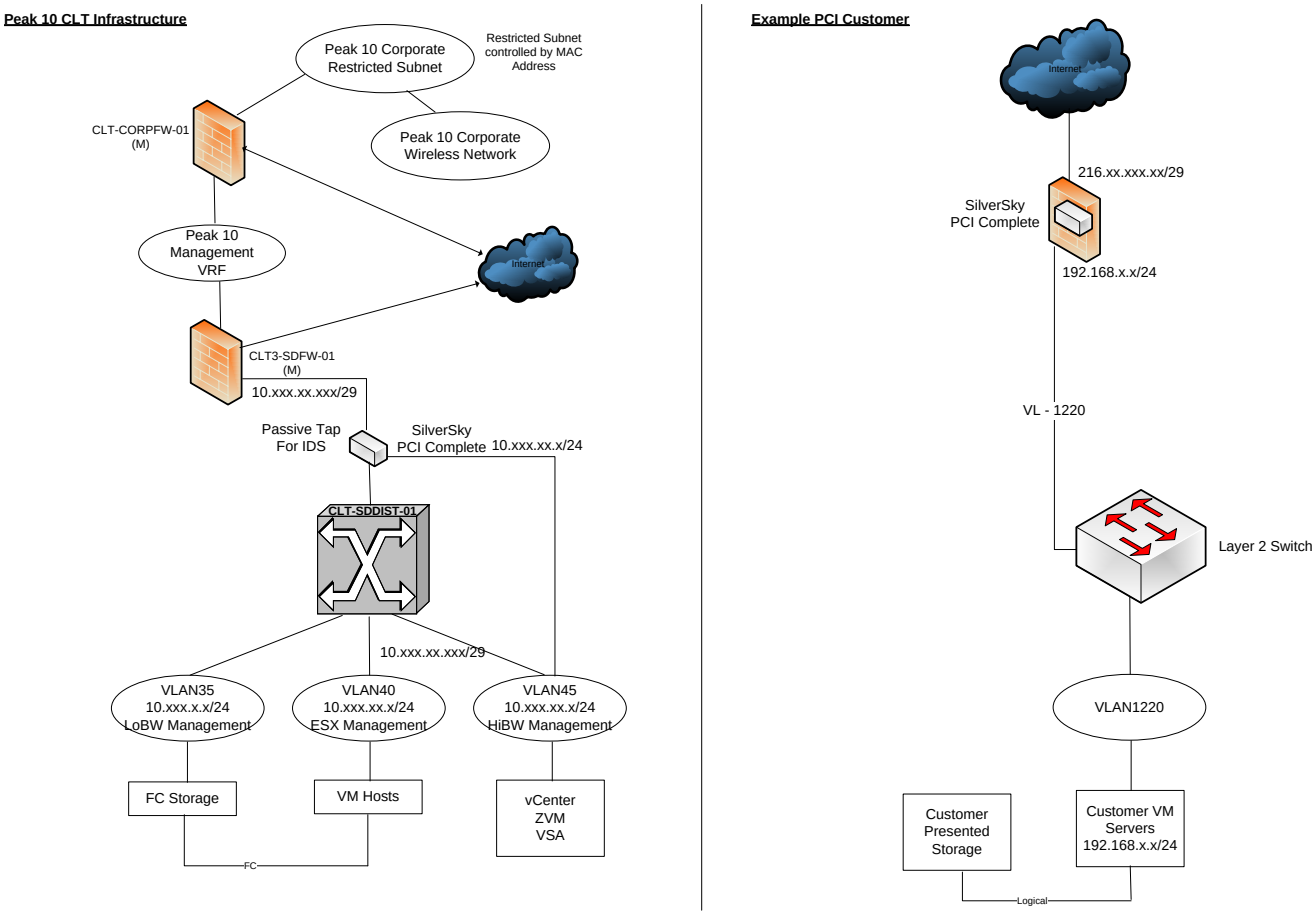
- Executive management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.

- Managed services – responsible for managing and protecting users' information and systems from unauthorized access and use while maintaining integrity and availability.
- Engineering – responsible for specifying, deploying and maintaining infrastructure systems, security, and support for user entities.
- Service delivery – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, delivering goods, and continued support.
- Marketing – responsible for marketing and sales functions.
- Operations – responsible for maintaining and operating data center infrastructure and user entities' IT environments in an efficient manner through the use of staff, resources, facilities, and business solutions.
- Finance and administration – responsible for providing financial and administrative support including HR, financial and regulatory reporting, banking, insurance, risk management, operational quality assurance and compliance and information systems related to financial reporting.

Procedures

Access Authentication and Authorization

The following outlines the connection to an example customer's virtual environment and the connection to the Peak 10 management network by Peak 10 personnel. All cloud data center locations were set up in the same manner. As noted above, the connection to the customer system, and the customer environment, were not included in this examination. Client cloud environments reside on private VLANs that are separate from other customers and Peak 10 networks.



Peak 10 support personnel access the management network infrastructure, utilizing the following steps:

1. Peak 10 support personnel connect to the Peak 10 corporate site either directly or remotely via encrypted VPN connections to the Peak 10 corporate network.
2. The service delivery firewalls allow only outbound traffic to the Internet and this traffic is restricted to only authorized subnets, IP addresses, and services. All inbound Internet access is routed through the corporate firewall.
3. Connection to the cloud service delivery network requires two-factor authentication using Fortigate RSA tokens via the Peak 10 corporate network. There are no externally facing devices in the cloud service delivery network. The corporate Fortigate firewall and the service delivery firewalls segment the corporate network from the cloud service delivery network.
4. Peak 10 management service delivery personnel authenticate to service delivery network devices via TACACS and to other systems via Active Directory.
5. The BAE Systems device collects logs from the cloud network delivery infrastructure and alerts Peak 10 personnel upon certain events.

Customers access their virtual environment via their own virtual switch and firewall, established and maintained by BAE Systems; however, this was not included in the scope of this examination.

Management network domain users are authenticated via a user account and password before being granted access to the network. Password parameters are enforced through a group policy on the managed services network and the network is configured to enforce the following password requirements:

- Minimum password length
- Password expiration intervals
- Invalid password account lockout threshold
- Password history
- Password complexity requirements

Administrative access privileges to the vCenter, vCommander, CommVault Simpana, and Cisco NX-OS systems are restricted to user accounts accessible by authorized personnel. Additionally, users are required to enter a user name and password to authenticate to these applications. Customer communications via the online vCommander portal are encrypted using Transport Layer Security (TLS).

A Fortigate stateful inspection, high-availability firewall system is in place at the network perimeter to filter unauthorized inbound traffic. This firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall ruleset. Any changes to the firewall configuration or rulesets are documented and approved by management in accordance with a predefined change management policy. Firewall rulesets are reviewed on a bi-annual basis. Certain firewall tasks that do not affect customers are considered “routine” and are thus pre-approved by management. These tasks as documented in a routine task policy document. The firewall system requires administrators to authenticate using an authorized user account and password prior to performing firewall administration tasks. Administrative privileges on the firewall system are restricted to the vice president of network and cloud infrastructure, regional manager of network engineering and network engineers. Additionally, users can only authenticate to the firewall from certain subnets, and the firewall system is configured to log a user out after a predefined period of inactivity.

Physical security requests (requests for badge access) are processed by users with administrative privileges to the badge access system. The ability to administer the badge access system is limited to authorized technical assistance center (TAC) personnel as described in the Physical and Environmental Security section below.

Access Requests and Access Revocation

Users are assigned access to the network based on groups in Windows Active Directory, and administrative privileges are restricted to user accounts accessible by authorized personnel, which include management and certain IT personnel. In order to be added to the management network or to be added to privileged groups on the network, a formal access request must be submitted via the ticketing system.

In order to ensure that the level of access requested is commensurate with the user's job responsibilities, the access request must be approved by the user's manager. The system administrators deactivate user accounts assigned to terminated employees as a component of the termination process. Infrastructure user account passwords are stored in an encrypted file that requires an authorized user account and password for access.

Requests to revoke badge access privileges are processed in a similar manner as a component of the employee termination process. Additionally, the compliance and security analyst performs a monthly review of badge access privileges for Peak 10 badge holders to help ensure terminated employees' access is revoked.

Antivirus

A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations by updating the antivirus definitions of registered clients on a daily basis and scanning those registered clients on a weekly basis.

Change Management - Infrastructure Change Control (Patching and Operating System (O/S) Change Management)

Policies and procedures are in place to guide personnel in documenting, scheduling, and performing infrastructure changes and maintenance activities. Requirements for performing infrastructure change management tasks include risk classifications, priority classifications, required documentation, approvals, and customer notifications. Operations and support personnel utilize the ServiceNow ticketing application to centrally track infrastructure change requests and maintenance activities. The standardized change management ticket includes, but is not limited to, the following:

- Individual requesting the change
- Description of the change and business reason
- The impact, complexity and derived risk rating associated with the change
- Affected facilities, systems and components

While completing the ServiceNow ticket, IT personnel judgmentally determine and select predefined impact and complexity level of the related change. ServiceNow will automatically calculate and generate a risk rating associated with the change. Certain routine changes, such as preventative maintenance activities, classified as "standard" are pre-authorized by the change advisory board (CAB) and do not require additional approval. Changes classified as "normal" or "emergency" may require functional and additional CAB approval based on the calculated risk level associated with the change and predefined approval requirements. Functional and CAB level approvals are documented and captured within the ServiceNow ticket.

Based on the impact and risk associated with a change, written customer notification may be required. The ServiceNow application will automatically generate and distribute the customer notifications based on the notification options selected during the creation of the change management ticket.

Physical and Environmental Security

Peak 10 data centers employ physical security controls to help ensure that only authorized personnel access the data centers. Documented physical security policies and procedures are in place to guide personnel in physical security administration as well as vendor administration procedures. Each data center is equipped with two separate two-factor authentication systems to control access. A combination of badge and PIN codes are required to enter the buildings while a badge and biometric fingerprint scan are required to enter the data centers. Visitors are required to sign a log at the front desk prior to entering the data centers and to be accompanied and supervised by a Peak 10 employee or an authorized client escort. Visitors are required to wear a visitor badge while visiting the data centers. Visitor badges do not allow unescorted access to the data centers. Technical assistance center (TAC) personnel are staffed at the data center facilities to log visitor access and monitor the digital surveillance systems at the data centers on a 24 hour basis.

Vendors who access the data center are required to sign a vendor accountability form in order to perform maintenance in the data centers, and vendor visits must be documented in a work order with a description of the issue, associated systems and steps taken to resolve the issue.

Administrator privileges to the badge access system are restricted to user accounts accessible by authorized facilities personnel, and badge access privileges of terminated employees are revoked as a component of the employee termination process. The compliance and security analyst reviews badge access system privileges on a monthly basis to help ensure that terminated employees have been deactivated within the badge access system.

Client equipment is maintained in lockable cages and racks within the data centers, and there are no exterior facing windows in the walls of the areas where client production servers are located.

Peak 10 has implemented and documented policies and procedures to ensure the environmental security of each data center. When a new data center is commissioned, management obtains a report from a third party specialist to ascertain that each new data center has been properly commissioned. These reports include reviews of project specifications and submittals, inspections of equipment installations, observations of original equipment manufacturer (OEM) startups and reviews of electrical and mechanical infrastructures.

Data centers are equipped with fire and smoke detectors which trigger visible and audible alarms in the event of a fire. Pre-action dry-pipe water sprinklers or agent-based fire suppression systems are present at each location along with hand-held fire extinguishers to allow for prompt suppression of fires. Management contracts with third party specialists to inspect the fire detection and suppression systems on an annual basis and the inspection reports are retained as evidence of completion. Facilities personnel inspect the hand-held fire extinguishers on a monthly basis, while a third party inspects the fire extinguishers on an annual basis. Documentation of each inspection is retained.

The data centers are equipped with multiple air conditioning units to regulate temperature and humidity. Management contracts with third party specialists to inspect the air conditioning units on a quarterly basis and the inspection reports are retained as evidence of completion. The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak. These water detection units are placed near the air conditioning units, either in drip pans or under the raised floor.

Each data center is equipped with fueled electric power generators and redundant UPS systems to provide continuous power in the event of an outage. The generators and UPS systems are each inspected for maintenance by a third party on a quarterly basis, and third party specialists perform quarterly load tests for the generators. Management obtains reports for completed maintenance activities and inspections.

Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including fire alarm status and suppression systems, temperature, humidity and air quality, power levels and availability. The environmental monitoring application is configured to notify operations personnel via on-screen or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems. Lastly, TAC personnel perform daily patrols to monitor and record readings from certain environmental equipment.

Data Backup and Disaster Recovery

For subscribing customers, Peak 10 provides a data backup solution. For these customers, full backups are performed on a weekly basis while incremental backups are performed on a daily basis. Engineering personnel are responsible for monitoring the status of backup jobs through automated notifications. And the backup system status notifications are available for subscribing customers through the customer web portal. In the event that a backup job fails multiple times, engineering personnel will investigate and resolve the issue via the incident management process. Peak 10 also provides optional tape rotation and electronic vaulting services to ensure recoverability of customer data in the event of a disaster. Peak 10 also provides tools for customers to manage their storage.

Peak 10 also performs backups over its internal managed services systems to ensure availability of systems and data in the event of an outage or disaster. Backups of managed services infrastructure are scheduled to occur on a daily incremental and weekly full basis.

Incident Response

As part of the Peak 10 managed storage solutions, an automated backup system is available for subscribing customers. A default backup configuration is utilized to perform system backups (full weekly and daily incremental backups). The backup system status notifications are available for subscribing customers through the web portal.

An automated issue management / ticketing system is utilized to document, prioritize, escalate and resolve problems affecting the services provided. The ticketing system is configured to include the incident date, time, summary, contact name, status, impact level, urgency, and associated service level agreement (SLA).

System Monitoring

Cloud, managed services, and network service levels are monitored by a dedicated Governance, Risk and Compliance group to ensure compliance with organizational policies and customer requirements. In addition, network operations personnel are scheduled to be available 24 hours per day to monitor and resolve problems affecting services provided. Incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating and resolving problems affecting managed and network services and include the following:

- Severity level definitions
- Escalation procedures
- Response time requirements for service alerts

An enterprise monitoring portal is available for subscribing customers. The monitoring application is configured to alert operations personnel via onscreen and e-mail alert notifications when certain predefined thresholds are exceeded on monitored systems. Performance metric and service level reports including availability, alert history, and trend analysis are available. The enterprise monitoring application is utilized to monitor the following:

- Availability of the network, host services and ports
- IP packet transmissions and latency
- Bandwidth utilization and performance
- CPU and hard disk utilization

Data

Various primary and supporting systems infrastructure data are analyzed and used to support Peak 10's Data Center Operations and Cloud Services system. Specific data includes, but is not limited to, the following:

- Activity logs of badge card and finger / hand print access attempts, including denied access attempts from the badge card access system and the biometric recognition access system.
- Alert notifications and monitoring reports generated from the network monitoring application and the data center environmental monitoring applications.
- Activity logs from the corporate firewalls, service delivery firewalls and routers and switches.
- Activity logs from the corporate firewalls and service delivery firewalls.
- Alert notifications of failed and successful data backups received from automated backup system.
- Incidents and issue reports documented within the automated ticketing system.

Additionally, an enterprise monitoring portal is available for subscribing customers. The customer portal is utilized to provide reporting information to customers for significant events related to the Data Center Operations and Cloud Services system.

The portal provides the following capabilities for Peak 10 customers:

- DNS administration

- Ticketing
- Alerts
- Maintenance calendar
- Server monitoring
- Backup reporting
- Bandwidth monitoring
- IP assignment reporting

Please refer to the" Infrastructure and Software" section above for more detailed descriptions of the types of inputs and outputs related to the primary and supporting systems infrastructure that support the Data Center Operations and Cloud Services system.

Customer data was not included in the scope of this examination.

Significant Changes During the Review Period

No significant changes to the Data Center Operations and Cloud Services system occurred during the review period.

System Boundaries

As outlined in the 2016 TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

The scope of the report is limited to the operations performed in the following data center facilities:

Market	Address
Atlanta	2775 Northwoods Parkway, Norcross, Georgia, 30071
	12655 Edison Drive, Alpharetta, Georgia, 30022
Charlotte	8910 Lenox Pointe Drive, Charlotte, North Carolina, 28273
	10105 David Taylor Drive, Charlotte, North Carolina, 28262
Cincinnati	5307 Muhlhauser Road, West Chester, Ohio, 45011
Jacksonville	4905 Belfort Road, Jacksonville, Florida, 32256
Louisville	752 Barret Avenue, Louisville, Kentucky, 40204
Nashville	7100 Commerce Way, Brentwood, Tennessee, 37027
	425 Duke Drive, Franklin, Tennessee, 37067
	4600 Carothers Parkway, Franklin, Tennessee, 37067
Raleigh	5150 McCrimmon Parkway, Morrisville, North Carolina, 27560
Richmond	8851-B Park Central Drive, Richmond, Virginia, 23227
South Florida	5301 NW 33rd Avenue, Fort Lauderdale, Florida, 33309
Tampa	9417 Corporate Lake Drive, Tampa, Florida, 33634

Market	Address
	8350 Parkedge Drive, Tampa, Florida, 33637

Subservice Organizations

The threat detection, log file monitoring and security scanning services (managed security monitoring services) provided by BAE Systems were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at BAE Systems, alone or in combination with controls at Peak 10, and the types of controls expected to be implemented at BAE Systems to meet those criteria.

Control Activity Expected to be Implemented by BAE Systems	Applicable Trust Services Criteria
BAE Systems is responsible for monitoring and reviewing intrusion detection system (IDS) security event logs and for notifying Peak 10 of critical events that require review and resolution.	CC5.1 CC6.1