System and Organization Controls (SOC) 2 Report

Security and Availability

Report on Rackspace's Description of its Dedicated Hosting Services System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to security and availability throughout the period October 1, 2019 to September 30, 2020

Prepared in Accordance with AT-C Section 205 pursuant to TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*

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

Table of Contents

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

I. REPORT OF INDEPENDENT SERVICE AUDITORS

To the Management of Rackspace Technology, Inc.

Scope

We have examined Rackspace Technology, Inc.'s ("Rackspace" or the "service organization") accompanying description of its Dedicated Hosting Services system (the "system") at the data centers specified in Exhibit I attached to Section II titled "Rackspace's Description of its Dedicated Hosting Services System" throughout the period October 1, 2019 to September 30, 2020 ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V, "Other Information Provided by Rackspace That is Not Covered by the Service Auditors' Report" is presented by Rackspace management to provide additional information and is not a part of the description. Information about Rackspace management's response to the control exception identified has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of controls to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service organization's responsibilities

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

Service auditors' responsibilities

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

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

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

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

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls

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

Opinion

In our opinion, in all material respects,

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

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

c. the controls stated in the description operated effectively throughout the period October 1, 2019

to September 30, 2020, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Rackspace, user entities of Rackspace's system during some or all of the period October 1, 2019 to September 30, 2020, business partners of Rackspace subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following ("specified parties"):

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

San Antonio, Texas
January 15, 2021

1 Fanatical Place
San Antonio, TX 78218

II. MANAGEMENT OF RACKSPACE'S ASSERTION

We have prepared the accompanying description of Rackspace's Dedicated Hosting Services system (the "system") at the data centers specified in Exhibit I titled "Rackspace's Description of its Dedicated Hosting Services System" throughout the period October 1, 2019 to September 30, 2020, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide user entities with information about the system that may be useful when assessing the risks arising from interactions with the system, particularly information about system controls that Rackspace has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* (AICPA, *Trust Services Criteria*).

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

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

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

c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria.

1 Fanatical Place
San Antonio, TX 78218

Exhibit I – In-scope Data Centers

The scope of this report pertains to the Dedicated Hosting Services at the following data centers:

- DFW3
- FRA1
- HKG1
- HKG5
- IAD3
- IAD4
- LON3
- LON5
- ORD1
- SYD2
- SYD4

III. RACKSPACE'S DESCRIPTION OF ITS DEDICATED HOSTING SERVICES SYSTEM

A. System Overview

Company Background

Rackspace Technology, Inc. ("Rackspace") began operations in December 1998 to provide managed web hosting services to businesses on tools including AWS, Google, VMware, Microsoft, Openstack®, and others. Today, Rackspace serves over 300,000 customers in 33 data centers worldwide. Currently, Rackspace employs over 6,500 people (Rackers) around the world.

Rackspace integrates industry leading technologies and practices for each customer's specific need and delivers it as a service via the company's commitment to Fanatical Experience®.

This report covers the Dedicated Hosting Services at the following data centers (in-scope data centers):

Data Center	Location	Ownership Type	Vendor
DFW3	Dallas, Texas	Leased	Digital Realty Trust
FRA1	Frankfurt, Germany	Leased	Digital Realty Trust
HKG1*	Hong Kong, China	Leased	PCCW Solutions
HKG5	Hong Kong, China	Leased	Digital Realty Trust
IAD3	Ashburn, Virginia	Leased	Digital Realty Trust
IAD4	Ashburn, Virginia	Leased	Equinix Limited
LON3	London, United Kingdom	Owned	Not applicable
LON5	London, United Kingdom	Leased	Digital Realty Trust
ORD1	Chicago, Illinois	Leased	Digital Realty Trust
SYD2	Sydney, Australia	Leased	Digital Realty Trust
SYD4	Sydney, Australia	Leased	Equinix Limited

*All customers and internal devices were migrated from HKG1 to HKG5 and the HKG1 data center was closed as of March 31, 2020. The description that follows and the detailed control objectives and control activities applicable to physical security for the leased data centers described in Section IV include the processes and controls that are applicable for the HKG5 data center for the period October 1, 2019 to September 30, 2020 and for the HKG1 data center for the period October 1, 2019 to March 31, 2020.

Rackspace owned data centers are those for which Rackspace does not utilize a vendor for any services.

Business Overview

Rackspace serves a broad range of customers with diverse hosting needs and requirements. Rackspace is segmented into business units. They include: Dedicated Hosting (Managed Hosting), Managed Colocation, Cloud, Fanatical Experience® for technologies, E-mail and Apps. Managed Colocation serves clients that have significant in-house expertise and only require support around physical infrastructure. Rackspace Hybrid Hosting offers a combination of hosting services that enables customers to use managed hosting and cloud services under one account. Rackspace Fanatical Experience® for technologies includes in-house expertise in support of AWS, VMware, Microsoft, OpenStack and others. Cloud Hosting serves clients scalable IT-enabled capabilities using Internet technologies.

Dedicated Hosting Services Overview

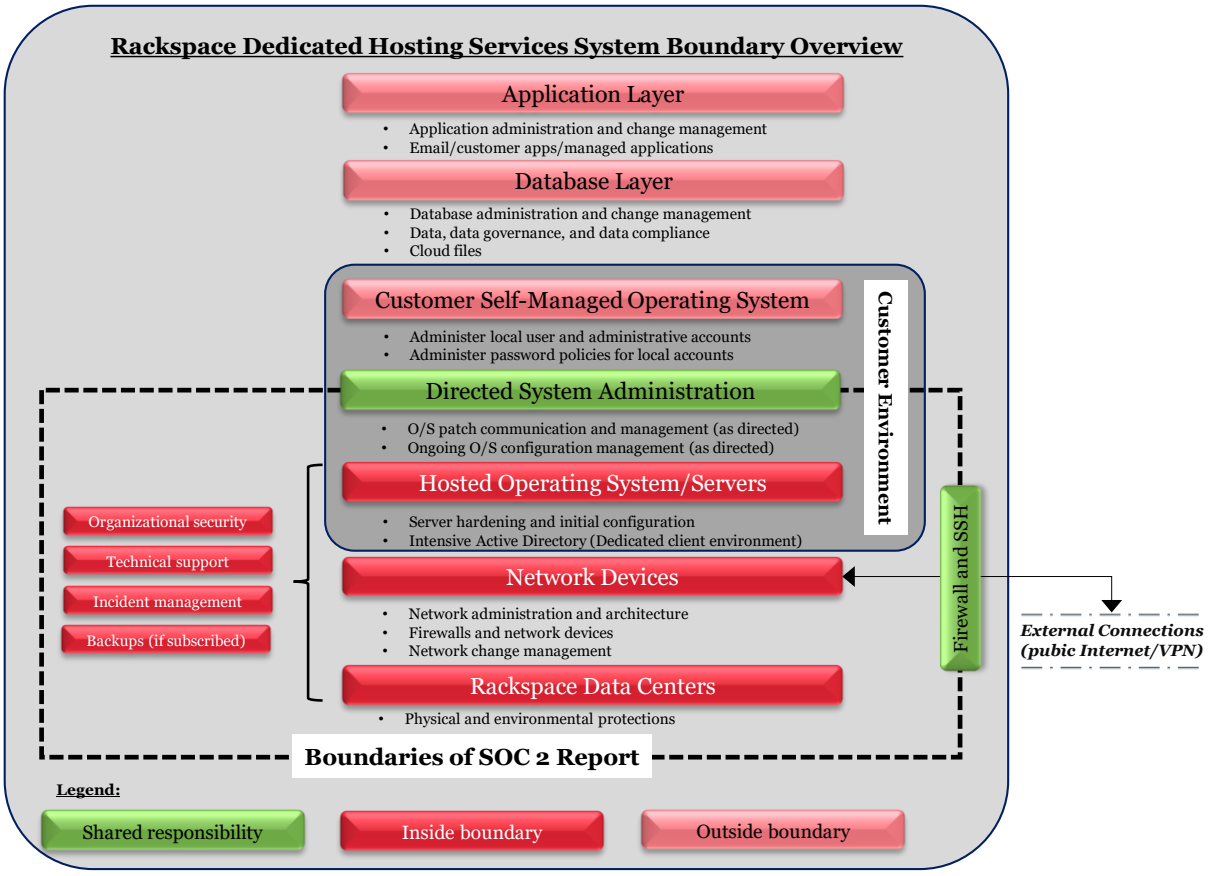
Dedicated Hosting Services come in the following forms:

- Dedicated Servers for high-performance workloads
- VMware managed environments
- Multi-cloud connectivity with scalability via third party cloud services
- Database management
- Dedicated DAS, SAN, Backup and NAS storage
- Secure network infrastructure management

Dedicated Hosting Services Boundaries and Scope of Report

This report includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the Dedicated Hosting Services system at Rackspace. This report does not extend to application and business process controls, automated application controls, or hosted application key reports that may be contained on servers hosted within the Dedicated Hosting Services system. Additionally, this report does not extend to the workloads (data, files, information) sent by Rackspace's customers to the Dedicated Hosting Services system. The integrity and conformity with regulatory requirements of such data are solely the responsibilities of the applicable Dedicated Hosting Services customer.

See the illustration below for a visual representation of the boundaries of the system and this report.



The boundaries for the data centers in scope include both owned and leased data center facilities. For the leased data center facilities (DFW3, FRA1, HKG1, HKG5, IAD3, IAD4, LON5, ORD1, SYD2, and SYD4),

Rackspace maintains direct monitoring controls, including annual risk assessments, a review of third-party reports, and periodic touchpoints with the operators of the data centers to provide coverage over the physical and environmental controls performed at those data centers.

The table below highlights the various elements associated with the boundaries of the Dedicated Hosting Services system.

Component	Datacenter / Hardware Locations	Network Device Platforms	Operating System Software	Customer Data and Applications
Dedicated Hosting Services	Corporate office locations: San Antonio, Texas Hayes, United Kingdom Owned data center Facility: LON3 Leased data center Facilities: DFW3, FRA1, HGK1, HKG5, IAD3, IAD4, LON5, ORD1, SYD2, and SYD4	• Brocade ADX • Cisco ASA Firewalls • F5 Networks Big-IP Firewalls • Cisco Routers • Cisco Catalyst Switches • Cisco Nexus Switches	• CentOS • ESXi • Red Hat Enterprise Linux • SUSE Linux • Ubuntu Linux • Windows Server O/S	Customer data and databases are solely the responsibility of Rackspace's customers and is not within the boundaries of the system. Customer applications and tools (including development and maintenance) are solely the responsibility of Rackspace's customers and are not within the boundaries of the system.

B. System Components

(1) Infrastructure

Overview

Rackspace manages and maintains infrastructure components supporting the Dedicated Hosting Services at the in-scope data centers. Rackspace is responsible for data center infrastructure services, including the following:

- Networking equipment (switches, routers, firewalls, load balancers),
- Physical and logical servers, and
- Physical and environmental security equipment at owned and operated data centers (cameras, badge readers, fire suppression).

Rackspace is responsible for Dedicated Hosting Services connectivity to the Internet. Rackspace is not responsible for connectivity from Rackspace's owned and leased data centers beyond this point. Rackspace data centers and Rackspace's Dedicated Hosting Services communicate between physical locations and data centers using secure protocols and links.

Network Device Platforms

Rackspace supports a large number of network devices that operate to support the Dedicated Hosting Services system. Network devices within the system boundaries include:

- Brocade ADX
- Cisco ASA Firewalls
- F5 Networks Big-IP Firewalls

- Cisco Routers
- Cisco Catalyst Switches
- Cisco Nexus Switches

Physical Access

As noted in the overview, Rackspace uses vendors that are responsible for the physical security controls at leased data centers. This description does not include the physical security controls performed by these vendors and is limited to monitoring controls performed by Rackspace.

Rackspace implements various physical security mechanisms to protect its personnel, hardware, network, and data from damage or loss due to unauthorized access. Controlled building access and secure access to specific areas are enforced through the administration of cards and biometric devices.

Documented physical security policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews physical security policies and procedures on an annual basis **(SOC 2.01)**. Physical access to data center facilities is documented and granted based on manager approval **(SOC 2.02)**. The vendor or Rackspace Data Center manager will revoke access when physical access is no longer needed due to termination of employment or services. For data centers except HKG5, physical access is disabled within 24 business hours of notification. For the HKG5 data center, physical access is disabled for terminated employees **(SOC 2.03)**.

Appropriateness of physical access to data center facilities is reviewed on a semi-annual basis **(SOC 2.04)** by Rackspace data center directors.

Access to Rackspace owned data centers is restricted through the use of biometric authentication devices (e.g. hand geometry and/or iris scanner) and key-card/badge devices. Personnel are required to display their identity badges when onsite at Rackspace facilities and visitors to the data center are required to be escorted at all times. Additional Physical safeguards are in place to restrict access to Rackspace owned data centers including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring **(SOC 2.05)**. Two factor authentication is used to gain access to each Rackspace owned data center **(GRP34)** and personnel are required to display their identity badges when onsite at Rackspace facilities.

Customers who are planning to visit a Rackspace data center facility are required to have a valid reason, valid government-issued ID, be approved by an authorized customer contact, and inform the Rackspace management team at least 72 hours prior to the data center visit. Rackspace personnel are on duty at Rackspace data center facilities 24 hours a day, seven days a week.

Environmental Controls

Environmental protections, software, and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet availability commitments and requirements. Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors where chilled water systems are used as coolant **(GRP59)**.

Data Center Operations utilize tools to monitor and evaluate environmental conditions and threats **(GRP78)**. These tools include fire detection and suppression systems to prevent and mitigate the risk of loss of data and equipment due to a fire. Additionally, data centers are equipped with uninterruptible power supplies (UPS) systems and diesel generators to mitigate data loss due to power failures and/or fluctuations.

(2) Software

Overview
Software systems are managed globally by Rackspace using consistent controls and processes. Rackspace utilizes a variety of software systems that supports the Dedicated Hosting Services system.

Operating Systems/Platforms
Rackspace supports a number of different operating systems as part of the Dedicated Hosting Services system. Platforms within the system boundaries include:

- CentOS
- ESXi (Virtual Host Operating System connected to VMWare stack for virtualized server infrastructure)
- Red Hat Enterprise Linux
- SUSE Linux
- Ubuntu Linux
- Windows Server O/S

Operational Support Tools
Rackspace operates several other tools that provide support to internal and customer systems. Such tools include:

- CORE – A custom developed system playing a critical service management and asset management repository role for Rackspace. All assets are tracked in CORE as well as critical security information (such as passwords for service accounts and other sensitive data regarding system configuration and management).

- SCCM (System Center Configuration Manager) – Microsoft product designed to manage configuration of system components.

- Spacewalk – configuration management tool utilized for Linux distributions.

- SUSE Manager – configuration and patch management tool utilized for SUSE Linux distributions.

- WSUS – patch management tool utilized for Windows servers.

Authentication/Authorization Services & Isolation Mechanisms
In supporting both the Dedicated Hosting Services system as well as providing support to Rackspace customers, Rackspace has implemented a series of tools that support authentication and authorization of individuals. Technologies within the system boundaries include:

- Active Directory – Rackspace utilizes Microsoft Active Directory to provide identity management via directory services for Rackspace employees as well as managing Microsoft server operating systems in the Dedicated Hosting Services system.

- Active Directory Federation Services (ADFS) – Standards-based service that allows the secure sharing of identity information between trusted business partners (federations) across an extranet.

- Cisco ACS – Cisco Access Control Server is Cisco's proprietary implementation of their authentication, authorization, and accounting tool for managing access to network components.

This is used as the primary means for access control in all Cisco networking devices in the Dedicated Hosting Services system (e.g., ASA firewalls, Catalyst/Nexus switches, routers).

- Sailpoint IdentityIQ (IIQ) – Governance-based Identity Access Management (IAM) solution that provides automated access certifications, policy management, access request and provisioning, password management, and identity intelligence.

- RSA – RSA Authentication Manager is utilized as the means to provide tokens with rolling PIN codes to enable multi-factor authentication where utilized in the Rackspace environment.

- NextGen Bastion Hosts – Balabit Shell Control Box appliances are utilized to provide application layer filtering and proxying of connections into in-scope environments, enforcing multi-factor authentication and creating isolation between in-scope and out-of-scope environments.

Security Tools

Multiple technologies are employed throughout the environment to enable information security controls and monitoring, including the following:

- Anti-virus/anti-malware – Rackspace employs Sophos A/V as the primary anti-malware technology on servers in the Dedicated Hosting Services system.

- CrowdStrike Falcon Intel – provides next-generation antivirus, endpoint detection and response, and cyber threat intelligence.

- Intrusion Detection System – Palo Alto network devices are utilized primarily to perform advanced traffic inspection (inclusive of both network layer and application layer inspection) to detect malicious attacks over network connections.

- Splunk – the primary source of log data and classified as Rackspace's central log repository, Splunk also functions as a Security Incident Event Management (SIEM) tool to correlate aggregated events and alert on suspected issues on an on-going basis.

Performance Monitoring Tools

Rackspace operates several tools for the purposes of monitoring systems and providing health checks across in-scope environments. The primary tool used within the system boundaries is:

- SCOM (System Center Operations Manager) – Microsoft product to support data center operational monitoring and maintenance of systems.

Other Tools and/or Services Supporting Infrastructure Components

Rackspace provides some tools and services for customers based upon their request and direction. Some of these tools include:

- MyRackspace Customer Portal – publicly facing web application where Rackspace customers may login to access account information regarding their Rackspace services as well as request updates to their environment (e.g. request firewall rule change, service request, configuration changes).

- Intensive Anti-Virus – customers may request that Rackspace install Sophos A/V agents on customer servers and provide on-going operational support for A/V solution.

- Managed Backup – The Managed Backup environment is a collection of servers in each data center utilized to provide data backup services for customers. The servers responsible for the primary service run the Commvault Simpana application and are referred to as a CommCell. The

process of data backup of a client is initiated by the CommServe (the central management server within a CommCell) via ServiceNet on a schedule, at which time the client negotiates a channel to the designated Media Agent and begins streaming data. The Media Agent (a server designed to transport data from client servers to target data storage) delivers the data across ServiceNet to the designated Isilon Network Attached Storage appliance.

- Managed Storage – Rackspace provides network attached storage in support of customers in virtualized environments as well as customers expanding storage requirements beyond their physical dedicated server offerings. Rackspace is not responsible for the encryption of any data at rest, and similar to Managed Backup, instruct customers that encryption of data at rest is the explicit responsibility of customers. Rackspace takes no responsibility over and does not explicitly monitor the data transferred to storage volumes.

- Segment Support Patching – Rackspace provides operating systems patching and update servers for supporting operating systems at the request of customers. Infrastructure including Red Hat Network servers, WSUS, SCCM, etc. are utilized by Rackspace to connect to systems at the request of customer and perform update operations. Customers are responsible for all validation of these activities in line with their compliance requirements.

- Rackspace Virtual Infrastructure - includes all management components of the virtualized infrastructure hosting service. This environment uses the VMware NSX Distributed Firewall to enforce strict isolation between components of the environment. There is a shared Management Plane (VMNet) network that connects Managed Hypervisors to this environment. Hypervisors have no IP connectivity to any other network segments. Hypervisors are additionally prohibited from communicating unnecessarily with each other on management interfaces. The above environment is deployed as a fully standalone environment across all Rackspace data centers, with lab/test environments also deployed as standalone, isolated, instances of this infrastructure. Access to the environment is supported via either RDP or SSH Bastion servers, which only allow access from the NextGen Bastion infrastructure. Once connected, engineers are able to connect to management interfaces on the vCenter Servers. For management, the vCenter servers connect to, and manage, hypervisors via a dedicated management network called VMNet. Devices on this network only have IP addresses to management interfaces, ensuring the management plane is fully isolated. Switch port ACLs on the ServiceNet switches also enforce separation of this network.

Logical Access to Network Infrastructure (Corporate Environment)

Rackspace takes measures to ensure employees with access to the network infrastructure have the appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself. Internal tools, resources, and equipment logically reside within the Corporate network. Access to these resources are limited to connections originating from within the network. Customer specific communications equipment represents the demarcation of shared infrastructure.

Independent domain controllers are in place for the administration and segregation of the Company's corporate network and customer environments. Access to the Company's network is restricted to authorized personnel only, and authentication mechanisms are in place to enforce such restrictions.

Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into each network. Access to the Rackspace network is restricted to authorized personnel only, and authentication mechanisms such as virtual private network (VPN) are in place to enforce such restrictions. Two-factor authentication is used to remotely connect to the Rackspace Corporate Network **(SOC 5.01)**. Access to VPN requires a unique pin and token.

The Technology and Engineering Services (TES) team is responsible for security administration functions, including the provisioning and deprovisioning of employee's logical access accounts in internal Rackspace systems.

The Global Data Center Infrastructure (GDCI) team administers the overall access to network infrastructure. Network infrastructure is categorized in two sets, Rackspace's network infrastructure (shared infrastructure) and customer's network infrastructure. The GDCI team manages Rackspace's network infrastructure, whereas the Network Security (NetSec) team manages the customer's network infrastructure.

The stability of the Rackspace network (shared infrastructure and customer infrastructure) is essential to meeting the company's delivery of uptime and reliability commitments to customers. Rackspace takes measures to ensure that all employees with access to the network infrastructure have the appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself.

Administrative access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services. Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS **(SOC 5.02)**. User activity is controlled and restricted by defining granular authorization privileges based on Corporate Active Directory groups.

Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system **(SOC 5.03)** that is compliant with the Rackspace Authentication Standard to further restrict access to the network. Splunk is configured to log multiple failed login attempts to the network **(GRP71)**.

New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval **(SOC 5.04)**. Human Resources is the only division authorized to request corporate network accounts for new employees. The request is initiated by adding a job position within the Global People System (GPS – HR database) to reflect the hire of a new employee. The Corporate Active Directory synchronizes with the GPS system every night to determine newly hired employees in need of a network account. Upon receiving Active Directory credentials, a new employee's manager is responsible for initiating an access request for any elevated or administrative access. Users request access to elevated or administrative rights through the SailPoint tool, which are then reviewed and approved/rejected. Following approval through SailPoint, an automated workflow will add users to the approved group, thereby allowing access.

In the event an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts the TES department to modify the transferred employee's access rights to those that are commensurate with the employee's new position and responsibilities.

Since administrative access to the network is granted and managed by adding the employee's network account into an AD group or several groups, management has implemented a process to review each of the members of a group by the group owner to ensure access is still appropriate. Users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed on a quarterly basis **(SOC 5.05)**.

The Corporate Active Directory – GPS synchronization also searches for terminated employees whose access needs to be removed from the network, supporting the timely removal of users with Active Directory access. Rackspace Corporate Active Directory access is disabled in a timely manner **(SOC 5.06)**.

Customer environments are isolated from one another via the use of VLAN to logically separate customer traffic **(SOC 5.07)**. Virtual networks (VLAN) are used to logically segment customers on the Rackspace

network into different broadcast domains to ensure packets are switched only between ports that are designated on the same VLAN, ensuring segmentation of networks amongst Rackspace customers.

In addition, there are several mechanisms and controls in place to safeguard network security and availability. For example, the ISOC team has implemented an intrusion detection system (IDS) to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks **(GRP41)**. Also, Rackspace has implemented an endpoint protection solution to monitor potential threats **(GRP39)**. Lastly, Rackspace has established a minimum baseline standard for servers and firewalls **(GRP76)**.

In addition to the above, the GES Cryptography Policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted **(GRP69)**. To reinforce the objective to secure data, the Secure File Transfer Standard and the Physical Media Handling Standard define mandatory security measures for when full encryption of removable media is required **(GRP40)**. Data sanitization occurs at the Rackspace owned data center LON3. For devices flagged for disposal or reuse at LON3, existing data is sanitized and evidence is retained **(GRP74)**.

Logical Access to Customer Environments

Employee access to customer environments is restricted through several layers of authentication mechanisms and systems. Systems restricting access to customer devices operate a role-based access functionality to provide appropriate segregation of duties within the company's workforce. CORE is the company's customer service platform, and while most of the Rackspace personnel have access to this system, only appropriate personnel have access to view sensitive information regarding customer devices.

Access to customer environments is restricted by allowing connections from bastion servers only **(SOC 6.03)**. The bastion server operates as a gateway and provides a layer of security between Rackspace infrastructure and the customer infrastructure; bastion servers enable the delivery of Rackspace services while protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific access group. Bastions provide security to customer environments by restricting access, ensuring the Rackspace infrastructure interfacing with the customer environment is secure. Rackspace personnel authenticate to a bastion server prior to authentication and connection to customer devices. Authentication to bastion servers requires a Racker to have an active account with the Corporate Active Directory.

Dedicated customer devices are managed within two forests, separate from the Rackspace Corporate Active Directory network domain:

- Intensive Active Directory: This multi-domain forest is used to authenticate Rackers into the dedicated customer environments. Certain customers utilize Intensive Active Directory to access their individual environment(s). Rackspace is continuing to transition these customers from Intensive Active Directory to the Global RS Active Directory.

- Global RS Active Directory: This single-domain forest is connected to the Intensive Active Directory and is used to authenticate customers into their individual environment(s). Global RS Active Directory consists only of customer accounts.

In order to access a customer environment, Rackers must have an active account within the Corporate Active Directory to access dedicated bastion servers. Then, utilizing their Intensive Active Directory credentials, Rackers can either access a customer environment within Intensive Active Directory or through a parent-child trust, within the Global RS Active Directory.

Customer environments are appropriately segregated from other customers through the use of Organizational Units within the Intensive and Global RS Active Directories **(SOC 6.01)**.

Rackspace has established a minimum password baseline configuration for its Intensive and Global RS Active Directory systems **(SOC 6.05)**. Also, Intensive Active Directory passwords used by Rackspace employees are configured to expire after a maximum of ten (10) hours **(SOC 6.02)**. Users with administrative privileges to customer devices are provisioned credentials within the Intensive Active Directory and specific Active Directory groups. New user accounts within Intensive Active Directory are created based on job function and/or manager approval **(SOC 6.04)**.

Users with administrative privileges to customer environments are frequently reviewed. Intensive Active Directory accounts are reviewed on a quarterly basis. Access identified for removal is completed in a timely manner **(SOC 6.07)**. Rackspace utilizes an in-house developed tool to automate certain review activities, including the initiation of the review and, for accounts marked for removal, automatically removing/disabling the access once the review is complete.

Individual Managed Hosting customer configurations utilize dedicated hardware for servers, firewalls, and load-balancers **(SOC 6.06)**. Dedicated managed hosting customers purchase hardware from Rackspace and are given read only access to allow full transparency into their own environment. Customer firewalls and other network devices delineate the boundary between Rackspace, customer environments, and shared infrastructure. Rackspace manages customer environments following strict security guidelines and policies as to not risk compromise of system and prevent overlap within the shared infrastructure. The customer is considered the primary system owner of their environment as changes are not made without their documented approval within a ticket. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment. A firewall rule set can be modified by authorized Rackspace employees with TACACS clearance which is checked by Cisco ACS software. All commands are authorized and accounted for via ACS.

Rackspace encrypts connections to Customer Portals using SSL or TLS **(GRP 24)**.

Incident Management

Rackspace has an incident response team responsible for the identification, tracking, documentation, resolution, and communication of incidents. The Incident Management Team facilitates the remediation and communication efforts for any incident affecting the company's products or infrastructure. Appropriate resources are rapidly engaged to help restore disrupted services and mitigate the possible adverse effects incidents can have on business operations. Leaders are provided with timely incident status information so they can make knowledgeable decisions and direct resources to maintain operations.

Incident response processes exist to respond to and document problems and incidents including security and operational disruptions, establish point(s) of contact and a threshold of incident levels, and are available to personnel through the intranet **(SOC 4.01)**.

The Global Security Operations Center (GSOC) has implemented several layers of security protection and defense mechanisms within the Rackspace network. The GSOC department is composed of three teams for proactive and reactive purposes: Defensive Infrastructure, Threat and Vulnerability Analysis (TVA) and Incident Response (IR). The Defensive Infrastructure team deploys GSOC security sensors and collectors throughout the network. This team monitors, maintains, and provides maintenance for all security equipment globally and ensures the GSOC is equipped to handle the latest threats based on emerging and existing technology. The Threat and Vulnerability Analysis Team is responsible for evaluating the infrastructure and operating systems that support internal applications for the services offered to customers. Additionally, the TVA team provides threat intelligence for the GSOC and Rackspace based on key relationships and vulnerability assessments performed throughout the year. Finally, the Incident Response team monitors, detects, and responds to cyber security events. The IR team proactively searches for malicious activity based on threat intelligence, investigates major events, and is responsible for educating all Rackers on safe and secure business practices.

The Incident Management Team manages the communication to Rackspace customers and employees regarding physical, network, and other incidents that could result in a degraded ability to service customers. Once an incident occurs, a ticket is created to track the event, a communication is sent to applicable Rackspace personnel and customers (as necessary), and upon resolution the ticket is closed. Escalation procedures are determined and communicated to the customer (as necessary) **(SOC 4.02)**. At a minimum, incident management event details include the impacted system, incident origin, incident start date and time, impact type (awareness, down, degraded), and severity level. Once an incident management event is created, a communication email is sent to applicable Rackspace personnel for notification and status update(s). When an incident is resolved, the ticket is closed documenting the time of the resolution. In the event of a customer impacting incident, escalation procedures are in place and communicated through the customer portal and/or other communication channels/processes, ensuring customers are notified and have increasing levels of authority to which to appeal.

Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities. Vulnerability scans of Rackspace infrastructure are performed in accordance with the defined security policy. Remediation plans are documented and tracked in accordance with the defined security policy **(GRP77)**.

An access control system is used to log administrator activity to network devices. Logged activity includes username, successful/unsuccessful login attempts, and timestamp. Logs are retained for one year and are available for review in case of an incident or suspicious activity **(GRP43)**.

Incidents that affect more than one customer or Rackspace operations (Enterprise Impacting) are managed from a centralized tool that provides alerting and escalation paths and procedures, communication procedures and command, control and communication across all Rackspace facilities.

Change Management

A structured change management process is documented within the Rackspace Technical Change Management Policy to prevent and reduce service disruptions of Rackspace's shared infrastructure due to changes such as upgrades, maintenances, and fine-tuning. Rackspace shared infrastructure represents any component of the communications network or physical environment that is not customer specific. Customer specific communications equipment represents the demarcation of shared infrastructure. This shared infrastructure is utilized by Rackspace customers to gain the economies of scale cost advantage benefits that shared infrastructure offers for applicable types of equipment. Examples include core routers, switches, hypervisors, SAN fabric, backup infrastructure, and Internet backbone connections.

A documented change management policy is in place and reviewed on an annual basis **(SOC 3.01)**. Infrastructure software and hardware changes are documented, undergo testing when technically feasible, and are approved prior to being migrated to production **(SOC 3.02)**.

Proposed changes to technical infrastructure are assessed to determine the level of approval and communication required before implementation. An assessment rating consists of the review of the change across five dimensions: potential impact, planned impact, resiliency, past history, and likelihood. Based on this assessment, a rating of High, Medium or Low is assigned. Technical infrastructure changes with a medium risk rank are escalated to the Change Sponsor for implementation approval, and technical infrastructure changes with a high-risk rank are escalated to the Change Sponsor and to the Change Management Board for implementation approval.

Proposed changes that are scored as high risk are presented and reviewed at the weekly Change Management Board Meeting. The Change Management Board approves high impact changes. From change inception to finalization, the Change Management Board works with relevant stakeholders to validate that potential interdependencies have been considered and appropriately addressed. Testing for changes is performed if technically feasible.

Rackspace customers are notified of changes in accordance with the Change Management Policy **(SOC 3.03)** via the customer portal and/or other communication channels/processes and are provided information on the effects of the changes to their operations so that they can take appropriate action. External customers are given at least 72-hours' notice for scheduled non-emergency and up to 72-hours' notice for emergency maintenances. Rackspace also communicates to customers the details regarding scheduled downtime emergency changes, and scheduled upgrades to application components (patches, service packs, utility software, etc.).

After the Change Management Board has reviewed changes and approved where necessary, the change is implemented. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the Change Management Board.

When vulnerabilities are identified, Rackspace categorizes the vulnerability based on risk and criticality. Critical patches are applied to systems in an as-needed, escalated timeframe. High and medium risk vulnerabilities are remediated during routine patching and maintenance cycles. Regardless of criticality, the patch is applied following the change management process described above and communicated to the customer via the customer portal and/or other communication channels/processes.

Internally, change requests are displayed on the ServiceNow (SNOW) maintenance calendar, which is visible to Rackspace employees **(GRP17)**. After the Change Board has reviewed changes and approved where necessary, technical infrastructure and hardware maintenance changes are migrated into the production environment. Unexpected issues or failures arising during, or identified following, the change implementation process is reported to Incident Management.

Availability

Processing capacity is monitored by data center personnel via the Data Center Operations Metrics dashboard **(GRP57)**. Data center capacity utilization is reviewed on a monthly basis by DC Leadership **(GRP58)**.

Capacity Management (power consumption) for customers is a single view of customer environments that concisely provides real time and trending information based on data gathered from the customer environment. The intent is to have the ability to provide a customer with a holistic view of their environment from network through storage to provide insight to the customer about where any potential capacity concerns in their environment may exist.

Rackspace utilizes redundant routing and switching equipment for its core network infrastructure **(GRP56)** to protect against availability issues. Rackspace internal policies and processes mandate that the use of resources shall be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.

Rackspace has developed and maintains a process to address its business continuity plan throughout the organization. This plan addresses the information security requirements needed for the Company's continuity in a disaster scenario. It plans for the maintenance and/or restoration of operations to ensure availability of information and continuity of critical business processes. More specifically, a Data Center business continuity plan (BCP) exists and provides the global business continuity plan for Rackspace Data Centers to manage significant disruptions to its operations and infrastructure **(GRP65)**.

Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements. Rackspace annually tests and updates its business continuity plans to confirm that they are up to date and effective **(GRP66)**. Tests include full walkthroughs of plans onsite to train staff on emergency events and to ensure plans are adequate in the case of an emergency. Tests are recorded, saved and used as learning exercises for future tests or emergencies.

Natural disasters have the potential to disrupt data centers and systems and data housed within these systems. Backups are scheduled and performed for customers who have subscribed to the backup services **(SOC 7.01)**. Backup utility software is used to schedule and perform backups of data on customer servers. Rackspace works with customers to establish a customized backup schedule that is specific to each customer's implementation and operations. In addition, the backup utility software performs backups according to the predefined schedule determined by the customer.

Backups of customer data for subscribed customers are completed as configured. Failures are monitored and alerts are configured to send to backup administrators **(SOC 7.02)**.

Periodic tests of the restoration process are performed at customer request for data restoration **(SOC 7.03)**. In the event of a data restoration request, the customer will create a ticket and specify the details of the data that is required to be restored. Upon successful completion of the restoration, the ticket is closed.

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace utilizes an automated disc failure alert process in order to mitigate the risk of faulty media **(GRP47)**. The backup utility software is configured to replace media after a set number of failed attempts to write to media.

(3) People

Organization and Management

In order to meet its commitments and requirements as they relate to security and availability, Rackspace has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. To that end, Rackspace maintains an organizational structure to properly note line of reporting within each department **(SOC ELC03)**.

Rackspace is segmented into business units. They include: Dedicated Hosting (Managed Hosting), Managed Colocation, Openstack Public Cloud, Rackspace Private Cloud, Fanatical Experience® for technologies, Managed Public Cloud, Rackspace Application Support, Rackspace Managed Security, E-mail and Apps. Each segment is led by a segment leader.

Ten global functions support these segments:

- Engineering
- Accounting & Finance
- Legal
- Employee Services
- Global Technical Support
- Global Data Center Infrastructure
- Sales & Marketing
- Information Technology
- Corporate Development/Strategy
- Global Enterprise Security

These global functions have been established to provide capabilities to complement the segments, and to realize economies of scale and quality control. The leaders of the various global functions, the segment leaders, and Corporate officers make up the Rackspace Leadership Team.

The Rackspace Leadership Team actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. Formal job descriptions exist for active and approved positions **(SOX ELC11)** and are effectively utilized and updated as needed.

The Board of Directors consists of members independent from management and has established sub-committees to provide oversight and monitoring of key risk areas (e.g., Audit Committee, Compensation Committee, and Compliance Committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives **(GRP72)**.

Human Resources (HR)

Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security and availability have the qualifications and resources to fulfill their responsibilities. Before hiring personnel, Rackspace takes actions to address risks to the achievement of objectives by making available the organizational values and behavioral standards in the Rackspace employee handbook.

Rackspace is committed to hiring and retaining talent to provide fanatical support. Management requires employees to be subjected to a background check during the hiring process **(SOC ELC04)**.

In connection with the application for employment, all prospective employees are required to authorize a background check by signing a release. This release allows Rackspace to request information for verification of background and personal character based on business necessity. The Rackspace pre-employment background check consists of four primary screens: identity, criminal, education, and employment. For criminal checks where permissible by law, 20 years for felonies and 10 years for misdemeanors are reviewed, as well as up to 10 years of previous employment history and verification of the highest level of education completed by the candidate. Current employees who are being considered for promotion or transfer may be subject to an additional background investigation. Background investigations may also be conducted as part of an internal investigation of alleged employee misconduct.

Employee competence is a key element of the control environment. Rackspace is committed to training and developing its employees. At least annually, the Human Resources Team/Management perform a review of key talent by individual and role to ensure that critical talent is retained and to ensure that the organizational structure is aligned in a way that will support the achievement of the Company's objectives and strategies **(SOX ELC01)**. Rackspace ensures that personnel have the knowledge and training needed to perform their duties. A formal management performance appraisal is documented and communicated to personnel each year **(SOX ELC09)**.

Codes of Conduct

Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability have the qualifications and resources to fulfill their responsibilities. Before hiring personnel, Rackspace takes actions to address risks to the achievement of objectives by making available the organizational values and behavioral standards in the Rackspace employee handbook. The employee handbook addresses the following topics: Personal Use of Rackspace or Customer Supplies and Equipment, Code of Business Conduct and Ethics, Internet Access Guidelines, and Employment Practices. The employee handbook is acknowledged by new hires **(SOC ELC01)**. In addition, Rackspace employees are trained on the Code of Business Conduct and Ethics annually **(SOC ELC02)**. Rackspace has implemented a Whistleblower Hotline and has communicated the hotline number to all employees **(GRP73)**.

(4) Procedures

Policies and Procedures

Rackspace management is responsible for directing and controlling operations and for establishing, communicating and monitoring policies, standards and procedures. Rackspace achieves operational and strategic compliance to the company's overall objectives through proper preparation, planning, execution and governance. The policies and procedures are a series of documents, which are used to describe the controls implemented within the Dedicated Hosting Services System. The purpose of the policies and procedures are to describe the environment and define the practices performed on behalf of the customer.

The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and Rackspace's commitments. Policies and procedures relevant to the Dedicated Hosting Services System have been included as part of the System Components.

Importance is placed on maintaining sound and effective internal controls and the integrity and ethical values of all Rackspace personnel. Rackspace takes actions to address risks to the achievement of these objectives by making available the organizational values and behavioral standards in the Rackspace Employee Handbook.

Rackspace promotes a culture based on core values defined by management and carried out by all Rackspace employees. These core values complement the company's ethical values, integrity model, professional conduct standards, and employee development pathways. The sum of these values and behaviors form Rackspace's unique environment by influencing the control consciousness of its employees.

Rackspace has assigned and delegated proper responsibilities and authority to members of the Company. Rackspace security and availability policies are in place and made available to employees **(GRP02)**.

Lastly, in order to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives, Rackspace maintains cyber, facility, and business interruption insurance policies **(GRP79)**.

Risk Management and Design and Implementation of Controls

Information Security Risk Assessments are completed by the Global Enterprise Security (GES) Governance Risk and Compliance team and require sign-off from leadership around the company. Leadership then makes decisions based on the evolving risk at the company. These decisions are communicated through the implementation of global strategies and process changes.

The Rackspace risk assessment process includes the identification, analysis, and management of risks that could impact the company's network infrastructure, application development, data management, and business operations. Rackspace recognizes its risk management methodology and processes as critical components of its operations to verify that customer assets are properly maintained. Rackspace incorporates risk management throughout its processes at both the corporate and segment levels.

Rackspace manages risks on an ongoing basis through a formal risk assessment process. The SOX Compliance Team performs a Financial and Fraud Risk Assessment during the annual planning/scoping process **(SOX ELC36)**. Additionally, the Global Enterprise Security Risk Management team identifies, assesses, prioritizes, and evaluates risk based on the Security Risk Management Plan. In addition to the formal risk assessment process, managers discuss and resolve issues as they arise within their areas. Also, managers monitor and adjust the control processes for which they are responsible on an as-needed basis.

This process is performed both informally and formally through regularly scheduled meetings and by the formation of a cross-functional team to manage Global Enterprise Security initiatives and projects. The ESWG (Enterprise Security Working Group) brings together members from various business units to discuss security risks, priorities and challenges. Additionally, the GES Risk Management team presents the company's top ten risks to the Internal Audit department and the Audit Committee for their review and consideration while developing their risk-based audit plan.

Rackspace in-house legal counsel reviews contracts and amendments with vendors and customers. Monitoring of performance against existing contracts with vendors and customers is a critical function performed by all of Rackspace's segments.

The Risk Management team evaluates the need for changes on a constant basis. This continuous evaluation serves to ensure Rackspace's commitment to security and availability of products and services. Rackspace has defined a risk assessment approach. A Security Risk Management Plan exists and provides

a methodology that defines Rackspace's risk assessment approach, how to identify risks, analyze and evaluate risk, and how to evaluate options for treatment of risks **(GRP19)**. Management identifies and rates risks. Identified risks are rated using a risk evaluation process and ratings per the Security Risk Management Plan. The Governance, Risk, and Compliance group identifies and evaluates enterprise risks on a continuous basis. Remediation plans are documented and tracked for risks that are rated higher than medium **(GRP20)**.

In addition, Rackspace identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security and availability. It reassesses risks and mitigation strategies based on the changes and the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.

A threat and vulnerability analysis team exists to identify any potential concerns that would impair system security **(GRP23)**.

Vendor Management

Rackspace maintains a vendor management program that includes the Supplier Relationship Management Policy and the Supplier Information Security Risk Management Program and Supplier Information Security Requirements Standards. Policy and Standards are reviewed and approved annually **(SOC ELC06)**.

In addition, at least annually Rackspace reviews third party assurance reports or performs a physical security and environmental controls onsite audit for each leased data center location **(SOC ELC08)**.

Communication

Rackspace management realizes that effective communication with personnel is vital in order to align Rackspace business strategies and goals with operating performance. Rackspace communicates its security and availability commitments to customers as appropriate. It also communicates those commitments and associated system requirements to internal employees to enable them to carry out their responsibilities. In addition to annual SOC 1, SOC 2 and SOC 3 reports, Rackspace communicates to internal parties the scope of systems through numerous compliance documents: PCI AOC, ISO 27001 Statement of Applicability, Rackspace Description of Controls, and Rackspace Dedicated FAQ **(GRP04)**.

So that users understand their role in the system and the results of system operation, information regarding system design and operation and boundaries has been prepared and communicated. Rackspace documents the data center(s) scope and boundaries through its Data Center Wiki. The DC Wiki is available to Rackspace employees through the Company's intranet. Data center policies, procedures, contact personnel and organization structure by region are also included **(GRP05)**. To ensure that employees understand the Rackspace commitment to security and their responsibilities to uphold that commitment, ongoing training is provided at least annually. Rackspace has instituted a Security Awareness Policy, and the workforce is trained on security expectations annually **(SOC 1.02)**. Security commitments are available to internal users on the company intranet and external customers **(SOC 1.03)**.

The Global Enterprise Security team releases periodic communications focusing on immediate security and availability issues and enhancements in security and availability products **(GRP06)**. An Information Security Policy is in place and available to personnel on the company intranet. Reviews are conducted at least annually and updates are performed as needed **(SOC 1.01)**.

Moreover, the Rackspace Chief Security Officer holds a "Town Hall" meeting at least quarterly with the Global Enterprise Security teams **(GRP11)** to discuss and communicate the department's goals and expectations. The intent is to ensure alignment, understanding, and communication on the Company's objectives globally. The meeting also serves as an opportunity for employees to express concerns and suggestions, or to ask questions relevant to the Company's objectives.

Security events, vulnerabilities, and any changes that could significantly affect the system of internal controls are communicated on a monthly basis to Rackspace Executive Leadership and Security Team **(GRP12)**.

Communication between Rackspace and external customers is essential to the delivery of Rackspace services, thus the Company's website hosts information pertaining to these services. The Rackspace Service Level Agreement (SLA) is communicated via the Company website and includes provisions for network, hardware, and infrastructure downtime, while the Rackspace Acceptable Use Policy (AUP) is available on the company website and lists activities not allowed by customers who are within the Rackspace network **(GRP10)**. Also, Rackspace's commitment regarding the system's security and availability is included in the Rackspace general terms and conditions which is available on the company website **(GRP08)**.

Rackspace communicates service commitments and system requirements to third parties through the Master Services Agreement, Managed Hosting Services Terms and Conditions, and the Hosted Information Addendum **(GRP70)**.

Monitoring of Controls

The design and operating effectiveness of controls are periodically evaluated against security and availability commitments and requirements, corrections, and other necessary actions relating to identified deficiencies are taken in a timely manner. Rackspace maintains formal incident response processes concerning both corporate network incidents and incidents affecting customer solutions. Monitoring is a critical aspect in evaluating whether controls are operating as intended and whether they are updated as necessary to reflect changes in the processes. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Appropriate levels of management review their Internal Controls frameworks on a quarterly basis and note any control weaknesses or material changes in controls/environment **(SOX ELC32)**.

Rackspace monitors compliance with leading security practices and internal security policies through the routine audits and assessment of its systems and processes. Assessments are performed following applicable industry standards and third-party audit firms are engaged in the assessment when appropriate. To complement these measures, exceptions to procedural problems are logged, reported, and tracked until resolved. Employee workstations are required to comply with security requirements outlined in the workstation security policy. Workstations are monitored for compliance to the defined security policy **(GRP75)**.

Rackspace monitors controls on an annual basis to ensure security and availability requirements are met. Non-conformities found are communicated with appropriate stakeholders in a timely manner and monitored **(GRP09)**. In addition, the controls environment is monitored on a quarterly basis by the SOX Team to ensure appropriate controls are in place. Control deficiencies are monitored to ensure appropriate actions are completed in a timely manner. Control deficiencies are reported to management **(SOX ELC28)**.

(5) Data

Data, as defined by Rackspace, constitutes the following:

- Data describing customer attributes
- HR Data supporting controls such as background checks
- Device configuration
- System files
- Error logs
- Access administration logs
- Electronic interface files

This report does not cover any customer data that is housed on Rackspace controlled infrastructure. Rackspace takes no responsibility for customer data on their systems and does not perform any control procedures to ensure that customer data is maintained completely and accurately.

In delivering these services, Rackspace has explicitly communicated to customers that Rackspace is not responsible for encryption of data as part of the Dedicated Hosting Services System. Further customers are instructed to ensure any data that may require encryption at rest be encrypted prior to backup and that encryption keys be stored in a manner such that Rackspace does not have access to the key.

C. Applicable Trust Services Categories and Criteria

Trust Services Categories

This report addresses the following categories as specified by the AICPA Trust Services Criteria:

- Security – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability of information or systems and affect the entity's ability to meet its objectives.

- Availability – Information and systems are available for operation and use to meet the entity's objectives.

Trust Services Criteria and Related Controls

Although the Trust Services Criteria and related controls are presented in Section IV of this report "Trust Services Categories, Criteria, Rackspace's Related Controls, and PricewaterhouseCoopers' Tests of Operating Effectiveness and Results of Tests", they are an integral part of Rackspace's description of the Dedicated Hosting Services system.

D. Applicable Trust Services Criteria not addressed within the scope of this report

All trust services criteria, within the scope of this report, are addressed by control activities.

E. Complementary User Entity Controls Relevant to the Security and Availability Criteria

Complementary user entity controls are not within the boundaries of the Dedicated Hosting Services system. The Dedicated Hosting Services system has been designed to include the controls necessary to achieve the relevant trust services criteria included in this report, as outlined in Section IV. As such, the boundaries of the Dedicated Hosting Services system do not extend to specific controls designed and implemented by user entities.

IV. TRUST SERVICES CATEGORIES, CRITERIA, RACKSPACE'S RELATED CONTROLS, AND PRICEWATERHOUSECOOOPERS' TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

The AICPA Trust Services Categories, criteria, Rackspace's related controls, and test results are included in this section. For each criteria, there is a description of the controls that are designed to meet the criteria. Also, PricewaterhouseCoopers LLP, Rackspace's independent service auditor, has performed testing of the controls and presents its findings.

Additionally, observation and inspection procedures were performed by PricewaterhouseCoopers LLP as it relates to system-generated reports, queries, and listings within management's description to assess the completeness and accuracy (reliability) of the information utilized in the performance of PricewaterhouseCoopers LLP's testing of the control activities.

Test Descriptions
Tests of the control environment, risk assessment, monitoring and information and communication included inquiry of appropriate management, supervisory and staff personnel, observation of Rackspace's activities and operations, and inspection of Rackspace's documents and records. The results of these tests were considered in planning the nature, timing and extent of PricewaterhouseCoopers LLP's testing of the controls designed to meet the criteria described on the following pages. Test procedures performed in connection with determining the operational effectiveness of Rackspace's controls:

Test	Description
Inquiry	Inquired of appropriate Rackspace personnel. Inquiries seeking relevant information or representation from Rackspace were performed to obtain, among other factors: • Knowledge and additional information regarding the control • Corroborating evidence of the control As inquiries were performed for substantially all Rackspace controls, this test was not listed individually in the tables in Section IV.
Observation	Observed the application or existence of specific controls as represented. This includes among other things: • Observation of the control owner performing the control • Observation of a control function
Inspection	Inspected documents and records indicating performance of the control. This includes among other things: • Inspection of management reports to assess whether items are properly monitored and resolved on a timely basis as required • Examination of source documentation and authorizations • Examining documents or records for evidence of performance
Reperformance	Reperformed the control or processing application to test the accuracy of its operation.

Security and Availability Criteria and Related Control Activity Mapping

Criteria Reference	Criteria Description	Control Reference
CC1.0 – Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	GRP72 SOC ELC01 SOC ELC06 SOX ELC09
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	GRP72
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	SOC ELC03 SOX ELC01
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	GRP02 SOC 1.02 SOC ELC01 SOC ELC04 SOX ELC01 SOX ELC09 SOX ELC11
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	GRP09 SOX ELC01 SOX ELC09
CC2.0 – Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	GRP09 GRP12 GRP39
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	GRP02 GRP04 GRP05 GRP06 GRP08 GRP10 GRP11 GRP12 GRP17 GRP72 GRP73 SOC 1.02 SOC 1.03 SOC 3.03 SOC 4.01 SOC ELC02 SOX ELC11

Criteria Reference	Criteria Description	Control Reference
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	GRP06 GRP08 GRP09 GRP10 GRP70 GRP73 SOC 1.03 SOC 3.03 SOC 4.01
CC3.0 – Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	GRP12 GRP19 GRP20 GRP72 SOX ELC01
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	GRP12 GRP19 GRP20 SOC ELC06
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	GRP19 GRP23 SOX ELC36
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	GRP12 GRP19 SOC ELC06
CC4.0 – Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	GRP09 SOC ELC08
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	GRP09 SOX ELC28 SOX ELC32
CC5.0 – Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	GRP09 GRP12 GRP20 SOX ELC28
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	GRP09 GRP12 GRP20 SOC 1.01
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	GRP09 GRP12 GRP20 SOC 1.01

Criteria Reference	Criteria Description	Control Reference
CC6.0 – Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	GRP34 GRP41 GRP69 SOC 1.01 SOC 5.01 SOC 5.02 SOC 5.03 SOC 5.04 SOC 5.05 SOC 5.07 SOC 6.02 SOC 6.03 SOC 6.04 SOC 6.05 SOC 6.06
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	SOC 5.04 SOC 5.05 SOC 5.06 SOC 6.04 SOC 6.07
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	SOC 5.02 SOC 5.04 SOC 5.06 SOC 6.01 SOC 6.04 SOC 6.07
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	SOC 2.01 SOC 2.02 SOC 2.03 SOC 2.04 SOC 2.05
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	GRP40 GRP74
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	GRP24 GRP41 GRP43 GRP71 SOC 5.01 SOC 5.03 SOC 5.07 SOC 6.03 SOC 6.05 SOC 6.06
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	GRP24 GRP40 GRP47 GRP69 GRP74

Criteria Reference	Criteria Description	Control Reference
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	GRP39 GRP41 GRP75 SOC 3.01
CC7.0 – System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	GRP41 GRP76 GRP77
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	GRP09 GRP12 GRP41 GRP43 GRP47 GRP71 GRP77
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	GRP06 GRP12 SOC 4.01 SOC 4.02
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	GRP12 GRP65 GRP66 GRP77 SOC 4.01 SOC 4.02
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	GRP65 GRP66 SOC 3.02 SOC 4.02 SOC 7.03
CC8.0 – Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	GRP12 GRP20 GRP76 SOC 3.01 SOC 3.02 SOC 3.03 SOC 4.01
CC9.0 – Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	GRP19 GRP20 GRP79
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	SOC ELC06 SOC ELC08

Criteria Reference	Criteria Description	Control Reference
Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	GRP57 GRP58 SOC 3.01
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	GRP47 GRP56 GRP59 GRP65 GRP78 SOC 4.02 SOC 7.01 SOC 7.02
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	GRP65 GRP66 SOC 7.03

Rackspace Control Activities

The following are the control activities designed and implemented within the Rackspace Dedicated Hosting Services System to meet the criteria relevant to security and availability, and PricewaterhouseCoopers' tests of operating effectiveness.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP02	Rackspace security and availability policies are in place and made available to employees.	Inspected the Rackspace security and availability policies to determine whether security and availability policies were in place. Inspected the Rackspace internal website to determine whether security and availability policies were made available to employees.	No exceptions noted. No exceptions noted.
GRP04	Rackspace communicates to internal parties the scope of systems through numerous compliance documents: PCI AOC, ISO 27001 Statement of Applicability, Rackspace Description of Controls, and Rackspace Dedicated FAQ.	Inspected the following compliance documents to determine whether the documents addressed the scope of systems: • PCI AOC • ISO 27001 Statement of Applicability • Rackspace Description of Controls • Rackspace Dedicated FAQ Inspected evidence to determine whether compliance documents were made available to internal parties.	No exceptions noted. No exceptions noted.
GRP05	Rackspace documents the data center(s) scope and boundaries through its Data Center Wiki. The DC Wiki is available to Rackspace employees through the Company's intranet. Data center policies, procedures, contact personnel and organization structure by region are also included.	Inspected the data center knowledge and community space (DC Wiki) to determine whether it was available to Rackers on the Company intranet. Inspected the DC Wiki to determine whether the scope and boundaries of the Rackspace Data center systems were documented and that it included policies, procedures, contact personnel and organization structure by region.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP06	The Global Enterprise Security team releases periodic communications focusing on immediate security and availability issues and enhancements in security and availability products.	For a sample of communications, inspected emails from Global Enterprise Security to determine whether the emails addressed immediate security and availability issues and enhancements in security and availability products.	No exceptions noted.
GRP08	Rackspace's commitment regarding the system's security and availability is included in the Rackspace general terms and conditions which is available on the company website.	Inspected the Company website to determine whether general terms and conditions were available. Inspected the general terms and conditions to determine whether Rackspace's commitment regarding the system's security and availability were included.	No exceptions noted. No exceptions noted.
GRP09	Rackspace monitors controls on an annual basis to ensure security and availability requirements are met. Non-conformities found are communicated with appropriate stakeholders in a timely manner and monitored.	Inspected the annual Internal Audit Compliance Schedule and Nonconformities tracking documents to determine whether Rackspace monitored controls. Inspected evidence to determine whether nonconformities were communicated.	No exceptions noted. No exceptions noted.
GRP10	The Rackspace Acceptable Use Policy (AUP) is available on the company website and lists activities not allowed by customers who are within the Rackspace network.	Inspected the Company website to determine whether the AUP was available. Inspected the Acceptable Use Policy (AUP) to determine whether the document specified activities not allowed by customers who are within the Rackspace network.	No exceptions noted. No exceptions noted.
GRP11	The Rackspace Chief Security Officer holds a "Town Hall" meeting at least quarterly with the Global Enterprise Security teams.	For a sample of Town Hall meetings, inspected evidence to determine whether attendees included members of the Global Enterprise Security teams.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP12	Security events, vulnerabilities, and any changes that could significantly affect the system of internal controls are communicated on a monthly basis to Rackspace Executive Leadership and Security Team.	For a sample of months, inspected evidence to determine whether security events, vulnerabilities, and any changes that could significantly affect the system of internal controls were communicated to Rackspace Leadership, Legal, and the Global Security team.	No exceptions noted.
GRP17	Change requests are displayed on the ServiceNow (SNOW) maintenance calendar, which is visible to Rackspace employees.	Inspected evidence to determine whether scheduled changes, which include technical infrastructure and hardware maintenance change requests, appeared within the ServiceNow (SNOW) maintenance calendar tool, which is visible to Rackspace employees.	No exceptions noted.
GRP19	A Security Risk Management Plan exists and provides a methodology that defines Rackspace's risk assessment approach, how to identify risks, analyze and evaluate risk, and how to evaluate options for treatment of risks.	Inspected the Security Risk Management Plan to determine whether it contained Rackspace's risk assessment approach, how to identify risks, how to analyze and evaluate risk, and how to evaluate options for treatment of risks.	No exceptions noted.
GRP20	The Governance, Risk, and Compliance group identifies and evaluates enterprise risks on a continuous basis. Remediation plans are documented and tracked for risks that are rated higher than medium.	For a sample of risk assessments rated higher than medium, inspected evidence to determine whether a remediation plan was documented and remediation activities were tracked.	No exceptions noted.
GRP23	A threat and vulnerability analysis team exists to identify any potential concerns that would impair system security.	Inspected an organizational chart of the Threat and Vulnerability Team to determine whether the team was organized and structured to identify any potential concerns that would impair system security. Inspected the Vulnerability Management Standard to determine whether the policy included steps for identifying potential concerns that would impair system security.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP24	Rackspace encrypts connections to Customer Portals using SSL or TLS.	Inspected the configuration of the Customer Portals to determine whether cryptography protocols such as SSL/TLS were in place.	No exceptions noted.
GRP34	Two factor authentication is used to gain access to each Rackspace owned data center.	Observed a Rackspace employee unsuccessfully access each owned data center without utilizing two factor authentication. Observed a Rackspace employee successfully access each owned data center utilizing two factor authentication.	No exceptions noted. No exceptions noted.
GRP39	Rackspace has implemented an endpoint protection solution to monitor potential threats.	For a sample of devices, inspected the configuration to determine whether endpoint protection is enabled on the device to protect against potential threats.	No exceptions noted.
GRP40	The Secure File Transfer Standard and the Physical Media Handling Standard define mandatory security measures for when full encryption of removable media is required.	Inspected the Secure File Transfer Standard and the Physical Media Handling Standard to determine whether the standards outlined the security measures for when full encryption of removable media is required.	No exceptions noted.
GRP41	The ISOC team has implemented an intrusion detection system (IDS) to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks.	Inspected a network diagram to determine whether an IDS was implemented on the Rackspace network. Inspected IDS configuration and an example alert to determine whether the IDS was configured to detect and act on the detection of anomaly network behavior.	No exceptions noted. No exceptions noted.
GRP43	An access control system is used to log administrator activity to network devices. Logged activity includes username, successful/unsuccessful login attempts, and timestamp. Logs are retained for one year and are available for review in case of an incident or suspicious activity.	Observed a failed login attempt to determine whether the activity was logged. Observed archived logs to determine whether logs are retained for at least one year.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP47	Rackspace utilizes an automated disc failure alert process in order to mitigate the risk of faulty media.	Inspected the SmartFail configuration to determine whether the tool was configured to automatically alert upon media failures. Observed the automated detection of an example media failure to determine whether SmartFail detected faulty media.	No exceptions noted. No exceptions noted.
GRP56	Rackspace utilizes redundant routing and switching equipment for its core network infrastructure.	Observed the use of routers for each Rackspace owned data center to determine whether Rackspace utilized redundant routing and switching equipment for its core network infrastructure. Inspected the Rackspace network diagram to determine whether there was redundant routing and switching equipment for the core network infrastructure.	No exceptions noted. No exceptions noted.
GRP57	Processing capacity is monitored by data center personnel via the Data Center Operations Metrics dashboard.	Inspected the Data Center Operations Metrics dashboard to determine whether the dashboard included details related to processing capacity at the data centers.	No exceptions noted.
GRP58	Data center capacity utilization is reviewed on a monthly basis by DC Leadership.	For a sample of months, inspected communications to determine whether data center capacity utilization was reviewed, the report was shared via the GDCI SharePoint site to data center leadership, and that the communication contained information regarding power utilization for each Rackspace owned data center.	No exceptions noted.
GRP59	Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors where chilled water systems are used as coolant.	Observed each Rackspace owned data center to determine whether they were equipped with sensors to detect environmental hazards.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP65	A Data Center business continuity plan (BCP) exists and provides the global business continuity plan for Rackspace Data Centers to manage significant disruptions to its operations and infrastructure.	Inspected evidence to determine whether a Data Center business continuity plan (BCP) exists and provided the global business continuity plan for Rackspace data centers to manage significant disruptions to its operations and infrastructure.	No exceptions noted.
GRP66	Rackspace annually tests and updates its business continuity plans to confirm that they are up to date and effective.	Inspected the business continuity plan testing log from the Rackspace GDCI wiki to determine whether business continuity plans were tested annually.	No exceptions noted.
GRP69	The GES Cryptography Policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted.	Inspected the GES Cryptography Policy to determine whether the policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted.	No exceptions noted.
GRP70	Rackspace communicates service commitments and system requirements to third parties through the Master Services Agreement, Managed Hosting Services Terms and Conditions, and the Hosted Information Addendum.	Inspected the Master Services Agreement, Managed Hosting Services Terms and Conditions, and the Hosted Information Addendum to determine whether the documents communicated security commitments and system operation responsibilities to third parties.	No exceptions noted.
GRP71	Splunk is configured to log multiple failed login attempts to the network..	Inspected system configurations to determine whether Splunk was configured to log multiple failed login attempts to the network.	No exceptions noted.
GRP72	The Board of Directors consists of members independent from management and has established sub-committees to provide oversight and monitoring of key risk areas (e.g., Audit Committee, Compensation Committee, and Compliance Committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives.	Inspected evidence to determine whether the Board of Directors consists of members independent from management. Inspected evidence to determine whether the Board of Directors has established sub-committees, each with a defined charter.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP73	Rackspace has implemented a Whistleblower Hotline and has communicated the hotline number to all employees.	Inspected the company intranet to determine whether the Whistleblower Hotline was implemented and communicated to employees.	No exceptions noted.
GRP74	For devices flagged for disposal or reuse at LON3, existing data is sanitized and evidence is retained.	For a sampled device flagged for disposal or reuse at LON3, determined through observation data was sanitized prior to disposal or reuse. For a sampled device flagged for disposal or reuse at LON3, inspected evidence to determine whether evidence was retained.	No exceptions noted. No exceptions noted.
GRP75	Employee workstations are required to comply with security requirements outlined in the workstation security policy. Workstations are monitored for compliance to the defined security policy.	Inspected the workstation security policy to determine whether guidelines related to workstation security compliance requirements were defined. For a sample of workstations, inspected evidence to determine whether workstations were monitored for compliance. For instances of non-compliance, inspected evidence that non-compliance has been remediated or an action plan exists.	No exceptions noted. No exceptions noted.
GRP76	Rackspace has established a minimum baseline standard for servers and firewalls.	Inspected the minimum baseline standard to determine whether it defined minimum baseline standards for servers and firewalls. Inspected system configurations to determine whether firewalls and servers are configured in adherence to the minimum baseline standard.	No exceptions noted. No exceptions noted.
GRP77	Vulnerability scans of Rackspace infrastructure are performed in accordance with the defined security policy. Remediation plans are documented and tracked in accordance with the defined security policy.	For a sample of vulnerability scans of Rackspace infrastructure, inspected evidence that the scans were executed in accordance with the defined security policy. Any vulnerabilities identified were tracked and remediation plans were documented.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP78	Data Center Operations utilize tools to monitor and evaluate environmental conditions and threats.	Observed monitoring tools and dashboards at each Rackspace owned data center to determine whether support tools monitored and evaluated environmental conditions and threats.	No exceptions noted.
GRP79	Rackspace maintains cyber, facility, and business interruption insurance policies.	Inspected the cyber, facility, and business interruption insurance policies to determine whether Rackspace insurance policies were in place.	No exceptions noted.
SOC 1.01	An Information Security Policy is in place and available to personnel on the company intranet. Reviews are conducted at least annually and updates are performed as needed.	Inspected the Information Security Policy to determine whether it was in place and available to personnel on the company intranet. Inspected evidence to determine whether the Information Security Policy was reviewed within the last year.	No exceptions noted. No exceptions noted.
SOC 1.02	Rackspace has instituted a Security Awareness Policy, and the workforce is trained on security expectations annually.	Inspected evidence that a Security Awareness Policy was in place. For a sample of employees, inspected evidence to determine whether the workforce was trained at least annually on security expectations.	No exceptions noted. No exceptions noted.
SOC 1.03	Security commitments are available to internal users on the company intranet and external customers.	Inspected evidence that security commitments were in place and available to internal users on the company intranet. Inspected evidence that security commitments were in place and available to external customers.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 2.01	Documented physical security policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews physical security policies and procedures on an annual basis.	Inspected the physical security policies and procedures to determine whether processes were in place to guide employees in the granting, controlling, and monitoring of physical access. Inspected evidence to determine whether the physical security policies and procedures were reviewed on an annual basis.	No exceptions noted. No exceptions noted.
SOC 2.02	Physical access to data center facilities is documented and granted based on manager approval.	For a sample of physical access granted to data center facilities, inspected evidence to determine whether physical access was documented and approved.	No exceptions noted.
SOC 2.03	<u>Data centers except HKG5:</u> Physical access is disabled within 24 business hours of notification. <u>HKG5 data center:</u> Physical access is disabled for terminated employees.	<u>Data centers except HKG5:</u> For a sample of terminated employees, inspected badge history within the badge access system to determine whether access was disabled within 24 business hours of notification. <u>HKG5 data center:</u> Inspected the full population of terminated employees and the listing of data center access to determine whether terminated users had access.	No exceptions noted. No exceptions noted.
SOC 2.04	Appropriateness of physical access to data center facilities is reviewed on a semi-annual basis.	For each in-scope data center facility, inspected evidence to determine whether a semi-annual review of appropriateness of physical access was performed; and if follow-up actions were requested, determined that they were completed.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 2.05	Physical safeguards are in place to restrict access to Rackspace owned data centers including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.	Observed an attempt to gain access to each owned data center without a proximity card. Observed an authorized individual access each owned data center with a proximity card. Observed the presence of physical safeguards outside the server room for each owned data center to determine whether access was appropriately restricted.	No exceptions noted. No exceptions noted. No exceptions noted.
SOC 3.01	A documented change management policy is in place and reviewed on an annual basis.	Inspected the Change Management Policy to determine whether it was in place and available to personnel on the company intranet. Inspected evidence to determine whether the Change Management Policy was reviewed on an annual basis.	No exceptions noted. No exceptions noted.
SOC 3.02	Infrastructure software and hardware changes are documented, undergo testing when technically feasible, and are approved prior to being migrated to production.	For a sample of changes, inspected evidence to determine whether changes were documented, tested when technically feasible, and approved prior to being migrated to production.	No exceptions noted.
SOC 3.03	Rackspace customers are notified of changes in accordance with the Change Management Policy.	For a sample of customer changes, inspected evidence to determine whether customers were notified of changes in accordance with the Change Management Policy.	No exceptions noted.
SOC 4.01	Incident response processes exist to respond to and document problems and incidents including security and operational disruptions, establish point(s) of contact and a threshold of incident levels, and are available to personnel through the intranet.	Inspected the incident management processes to determine whether processes were in place, established point(s) of contact and thresholds of incident levels, and were available to personnel through the intranet.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 4.02	Once an incident occurs, a ticket is created to track the event, a communication is sent to applicable Rackspace personnel and customers (as necessary), and upon resolution the ticket is closed. Escalation procedures are determined and communicated to the customer (as necessary).	For a sample of incidents, inspected the corresponding incident ticket to determine whether a ticket was created to track the event, a communication was sent to applicable Rackspace personnel and customers (as necessary), and the ticket was closed upon resolution.	No exceptions noted.
SOC 5.01	Two-factor authentication is used to remotely connect to the Rackspace Corporate Network.	Observed a Rackspace employee unsuccessfully connect to the Rackspace Corporate Network without utilizing two-factor authentication. Observed a Rackspace employee successfully connect to the Rackspace Corporate Network utilizing two-factor authentication. Inspected the configuration that requires users to authenticate through a VPN.	No exceptions noted. No exceptions noted. No exceptions noted.
SOC 5.02	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS.	For a sample of customer firewalls, inspected the firewall configuration and determined whether inherent access control functionality in Cisco ACS was utilized.	No exceptions noted.
SOC 5.03	Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system.	Inspected the Default Domain Policy and compared it to Rackspace's Authentication Standard to determine whether Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system.	No exceptions noted.
SOC 5.04	New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval.	For a sample of new administrators, inspected evidence to determine whether access was based on job function and manager approval.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 5.05	Users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed on a quarterly basis.	For a sample of quarterly reviews of users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations, inspected evidence to determine whether the review was performed and follow-up actions were completed.	No exceptions noted.
SOC 5.06	Rackspace Corporate Active Directory access is disabled in a timely manner.	For a sample of terminated employees, inspected access logs to determine whether the users' access was disabled timely.	No exceptions noted.
SOC 5.07	Customer environments are isolated from one another via the use of VLAN to logically separate customer traffic.	For a sample of customer firewalls, inspected the VLAN configuration to determine whether VLANs were utilized to logically separate customer traffic.	No exceptions noted.
SOC 6.01	Customer environments are appropriately segregated from other customers through the use of Organizational Units within the Intensive and Global RS Active Directories.	For a sample of customers, inspected the customer organizational units and determined whether units are appropriately segregated from other customers within Intensive and Global RS Active Directories.	No exceptions noted.
SOC 6.02	Intensive Active Directory passwords used by Rackspace employees are configured to expire after a maximum of ten (10) hours.	Observed a Rackspace employee check out an Intensive Active Directory account to determine whether the account was set to expire after ten (10) hours. Observed a password for a sampled account expire to determine whether the user could no longer access the account.	No exceptions noted. No exceptions noted.
SOC 6.03	Access to customer environments is restricted by allowing connections from bastion servers only.	For a sample of customer firewalls, inspected the firewall configuration to determine whether access was administered by allowing connections from bastion servers only.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 6.04	New user accounts within Intensive Active Directory are created based on job function and/or manager approval.	For a sample of new user accounts within Intensive Active Directory, inspected evidence to determine whether new accounts were created with manager approval.	No exceptions noted.
SOC 6.05	Rackspace has established a minimum password baseline configuration for its Intensive and Global RS Active Directory systems.	Inspected the password configuration settings for Intensive and Global RS Active Directories to determine whether a minimum password baseline was configured.	No exceptions noted.
SOC 6.06	Individual Managed Hosting customer configurations utilize dedicated hardware for servers, firewalls, and load-balancers.	For a sample of customers, inspected the corresponding CORE ticket to determine whether customers had dedicated infrastructure (hardware for servers, firewalls, and load-balancers).	No exceptions noted.
SOC 6.07	Intensive Active Directory accounts are reviewed on a quarterly basis. Access identified for removal is completed in a timely manner.	For a sample of quarterly reviews of users with access to Intensive Active Directory, inspected evidence to determine whether the review was performed; and if follow-up actions were requested, inspected evidence to determine that they were completed.	**Exception noted.** Five (5) out of five (5) follow-up actions sampled for the Q2 review were not completed due to a system bug.
SOC 7.01	Backups are scheduled and performed for customers who have subscribed to the backup services.	For a sample of customers subscribed to backup service, inspected evidence that customer data was configured in the backup management system.	No exceptions noted.
SOC 7.02	Backups of customer data for subscribed customers are completed as configured. Failures are monitored and alerts are configured to send to backup administrators.	For a sample of dates and customers, inspected evidence that backups were successful based on configured frequency or failures were resolved. Inspected the configuration of the backup management system to determine whether backup failures were configured to send alerts to backup administrators.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 7.03	Periodic tests of the restoration process are performed at customer request for data restoration.	For a sample of customer restoration requests, inspected evidence to determine whether the restorations were completed successfully or appropriately actioned upon.	No exceptions noted.
SOC ELC01	The employee handbook addresses the following topics: Personal Use of Rackspace or Customer Supplies and Equipment, Code of Business Conduct and Ethics, Internet Access Guidelines, and Employment Practices. The employee handbook is acknowledged by new hires.	Inspected the Rackspace employee handbook to determine whether the following topics were addressed: (1) Personal Use of Rackspace or Customer Supplies and Equipment, (2) Code of Business Conduct and Ethics, (3) Internet Access Guidelines, and (4) Employment Practices. For a sample of new hires, inspected evidence that new hires acknowledged receipt of the handbook.	No exceptions noted. No exceptions noted.
SOC ELC02	Rackspace employees are trained on the Code of Business Conduct and Ethics annually.	For a sample of employees, inspected the annual Code of Conduct and Ethics testing results from the Learning Management System (LMS) to determine whether Rackspace employees were trained on the Code of Business Conduct and ethics during the last 12 months.	No exceptions noted.
SOC ELC03	Rackspace maintains an organizational structure to properly note line of reporting within each department.	Inspected the Organizational Directory to determine whether the organization structure was maintained and included lines of reporting and job responsibilities.	No exceptions noted.
SOC ELC04	Management requires employees to be subjected to a background check during the hiring process.	For a sample of new hires, inspected evidence to determine whether background checks were performed.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC ELC06	Rackspace maintains a vendor management program that includes the Supplier Relationship Management Policy and the Supplier Information Security Risk Management Program and Supplier Information Security Requirements Standards. Policy and Standards are reviewed and approved annually.	Inspected the Supplier Relationship Management Policy, the Supplier Information Security Risk Management Program, and the Supplier Information Security Requirements Standard to determine whether policies and standards were in place. Inspected evidence to determine whether the Supplier Relationship Management Policy, the Supplier Information Security Risk Management Program, and the Supplier Information Security Requirements Standard were reviewed on an annual basis.	No exceptions noted. No exceptions noted.
SOC ELC08	At least annually Rackspace reviews third party assurance reports or performs a physical security and environmental controls onsite audit for each leased data center location.	Inspected evidence for each leased data center to determine whether Rackspace obtained third party assurance reports or performed a Physical Security and Environmental on-site audit annually. For a sample of data centers, inspected evidence to determine whether Rackspace performed an assessment over the leased data center within the last year.	No exceptions noted. No exceptions noted.
SOX ELC01	At least annually, the Human Resources Team/Management perform a review of key talent by individual and role to ensure that critical talent is retained and to ensure that the organizational structure is aligned in a way that will support the achievement of the Company's objectives and strategies.	For a sample of employees, inspected evidence to determine whether the Human Resources Team/Management performed a review of key talent by individual and role.	No exceptions noted.
SOX ELC09	A formal management performance appraisal is documented and communicated to personnel each year.	Inspected evidence to determine whether a formal management performance appraisal was documented and communicated to personnel annually.	No exceptions noted.
SOX ELC11	Formal job descriptions exist for active and approved positions.	For a sample of active and approved positions, inspected evidence to determine whether formal job descriptions exist.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOX ELC28	Controls environment is monitored on a quarterly basis by the SOX Team to ensure appropriate controls are in place. Control deficiencies are monitored to ensure appropriate actions are completed in a timely manner. Control deficiencies are reported to management.	For a sample of quarters, inspected evidence to determine whether the controls environment was monitored by the Rackspace SOX Team and control deficiencies were monitored, actions were completed in a timely manner, and were reported to management.	No exceptions noted.
SOX ELC32	Appropriate levels of management review their Internal Controls frameworks on a quarterly basis and note any control weaknesses or material changes in controls/environment.	For a sample of quarters, inspected evidence to determine whether management reviewed their Internal Controls framework and noted any control weaknesses or material changes in controls/environment.	No exceptions noted.
SOX ELC36	The SOX Compliance Team performs a Financial and Fraud Risk Assessment during the annual planning/scoping process.	Inspected evidence to determine whether the Financial and Fraud Risk Assessment was completed during the annual planning/scoping process.	No exceptions noted.

V. OTHER INFORMATION PROVIDED BY RACKSPACE THAT IS NOT COVERED BY THE SERVICE AUDITORS' REPORT

The information in this section describing management's response to the exceptions noted is presented by Rackspace to provide additional information to its users and is not part of Rackspace's description of controls that may be relevant to the users. Such information has not been subjected to the procedures applied in the examination of the description of Rackspace's operations on behalf of its users, and accordingly, the Service Auditor expresses no opinion on it.

Management's Response to Exceptions

Ref	Results of Test(s)	Management's Response to Exceptions
SOC 6.07	Five (5) out of five (5) follow-up actions sampled for the Q2 review were not completed due to a system bug.	Management has identified these additional factors associated with this control exception: • Management independently identified the system bug and implemented a fix prior to the next quarterly review cycle. • Management has automated processes that facilitates a comprehensive quarterly review of accounts that require access to customer environments. • Management determined that the root cause of the follow-up actions not being completed was due to a bug that went undetected that prevented the automated processing of account disable/removal. • Management reviewed logs for the previous 2019 and 2020 reviews and confirmed that the bug impacted the Q2 2020 instance only. • Management implemented the bug fix in Q3 2020 through code changes which followed the standard change control process, including testing and code review. • Management performed a comprehensive review during the Q3 2020 instance and confirmed that processes were completed successfully after the required code changes were implemented. • Additional validation planned by Rackspace Management in Q1 2021 to ensure the review is completed successfully and integrity of the review is maintained by increasing visibility through notifications for discrepancies in the total number of accounts processed.

(This page has been intentionally left blank.)