Service and Organization Controls (SOC) 2 Report
Security and Availability

Report on Rackspace's Description of its Data Center Services System and on the Suitability of the Design and Operating Effectiveness of Controls to meet the criteria for the security and availability principles throughout the Period November 1, 2016 to October 31, 2017

Prepared in Accordance with AT-C 205 pursuant to TSP Section 100A: *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)*

Table of Contents

I. Report of Independent Service Auditors

To the Management of Rackspace US, Inc. ("Rackspace")

Scope

We have examined the accompanying description titled "Rackspace's Description of the Data Center Services System"[1] (the "description") throughout the period November 1, 2016 to October 31, 2017 based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)* ("applicable trust services criteria"), throughout the period November 1, 2016 to October 31, 2017.

Service organization's responsibilities

In Section II, Rackspace has provided the accompanying assertion titled "Management of Rackspace's Assertion Regarding the Data Center Services System Throughout the Period November 1, 2016 to October 31, 2017," ("assertion") about the fairness of the presentation of the description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Rackspace is responsible for (1) preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; (2) providing the services covered by the description of the service organization's system; (3) selecting the trust services principles addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) identifying any applicable trust services criteria related to the principles being reported on that have been omitted from the description and explaining the reason for the omission, and (6) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditors' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period November 1, 2016 to October 31, 2017.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria involves

1 The scope of this report pertains to the Dedicated Hosting business services only.

- performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria and the controls were suitability designed and operating effectively to meet the applicable trust services criteria throughout the period November 1, 2016 to October 31, 2017.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

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

Opinion

In our opinion, in all material respects, based on the description criteria identified in Rackspace's assertion and the applicable trust services criteria

a. the description fairly presents the system that was designed and implemented throughout the period November 1, 2016 to October 31, 2017.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 1, 2016 to October 31, 2017.

c. the controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period November 1, 2016 to October 31, 2017.

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 Data Center Services system during some or all of the period November 1, 2016 to October 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators (collectively referred to as "specified parties") who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization;
- How the Service Organization's system interacts with user entities, subservice organizations, and other parties;
- Internal control and its limitations;

- User entity responsibilities, complementary user entity controls, and how they interact with related controls at the Service Organization and subservice organizations to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten meeting the applicable trust services criteria and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties. 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 29, 2018

II. Rackspace's Assertion

Management of Rackspace's Assertion Regarding the
Data Center Services System Throughout the Period November 1, 2016 to October 31, 2017

We have prepared the accompanying description titled "Rackspace's Description of the Data Center Services System" (the "description") throughout the period November 1, 2016 to October 31, 2017, based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about Rackspace's Data Center Services system, particularly system controls intended to meet the criteria for the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)* ("applicable trust services criteria").We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the Data Center Services system throughout the period November 1, 2016 to October 31, 2017, based on the following description criteria:

   i The description contains the following information:

      (1) The types of services provided

      (2) The components of the system used to provide the services, which are as follows:

         (a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

         (b) Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

         (c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

         (d) Procedures. The automated and manual procedures.

         (e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

      (3) The boundaries or aspects of the system covered by the description

      (4) For information provided to, or received from, subservice organizations and other parties[2]

         (a) how the information is provided or received and the role of the subservice organizations and other parties

         (b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

      (5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

         (a) Complementary user entity controls contemplated in the design of the service organization's system[3]

2 Subservice organizations were not relevant achieve the applicable trust services criteria. Therefore, this description criteria is not applicable.
3 Complementary user entity controls are not applicable for the system. Therefore, this description criteria is not relevant.

(b) When the inclusive method is used to present a subservice organization, controls at the subservice organization[2]

(6) If the service organization presents the subservice organization using the carve-out method[2]

(a) the nature of the services provided by the subservice organization

(b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(7) Any applicable trust services criteria that are not addressed by a control and the reasons

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description

ii The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed to meet the applicable trust services criteria throughout the period November 1, 2016 to October 31, 2017.

c. the controls stated in the description operated effectively throughout the period November 1, 2016 to October 31, 2017, to meet the applicable trust services criteria.

III. Rackspace's Description of the Data Center Services System

A. System Overview

Company Background

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

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

Data Center Services 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;
- Hybrid Hosting;
- Cloud, Fanatical Support® for technologies; and
- 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 Support® for technologies includes in-house expertise in support of AWS, VMware, Microsoft, OpenStack and others. The scope of this report only pertains to the Dedicated Hosting business services and not the other services.

Data Center Services Boundaries and Scope of Report

This report includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the Data Center Services System.

This report does not extend to application and business process controls, automated application controls, or hosted application key reports that may be contained within the data center services boundaries. Additionally, this report does not extend to the workloads (data, files, information) sent by Rackspace's customers to the Data Center Services System. The integrity and conformity with regulatory requirements of such data are solely the responsibilities of the applicable Data Center Services customer.

The system boundaries relating to this SOC 2 report start at the edge/entry point of the network and extend through the corporate network domain and includes the dedicated infrastructure environment.

This report is limited to the Data Center Services across various office locations (San Antonio, Texas and Hayes, United Kingdom), the Rackspace owned (DFW1, LON3) data center facilities, and the leased data center facilities (ORD1, IAD2, IAD3, DFW2, DFW3, LON5, HKG1, SYD2, SYD4, FRA1).

For the leased data center facilities (ORD1, IAD2, IAD3, DFW2, DFW3, LON5, HKG1, SYD2, SYD4, and FRA1), 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.

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

The table below highlights the various elements associated with the boundaries of the Data Center Services system.

Component	Datacenter / Hardware Locations	Network Device Platforms	Operating System Software	Customer Data and Applications
Data Center Services	Corporate office locations: San Antonio, TX Hayes, United Kingdom Owned data center Facilities: DFW1, LON3 Leased data center Facilities: ORD1, IAD2, IAD3, DFW2, DFW3, LON5, HKG1, SYD2, SYD4, FRA1	• 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 is 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 Data Center Services at a number of data center facilities around the world. 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 data centers (cameras, badge readers, fire suppression).

Rackspace is responsible for Data Center Services connectivity to the Internet. Rackspace is not responsible for connectivity from Rackspace's owned and leased data centers beyond this point. Rackspace datacenters and Rackspace's Data Center 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 Data Center Services systems. 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

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.

Access to the data center is restricted through the use of biometric authentication devices (e.g. hand geometry scanner) and key-card/badge devices. Two-factor authentication is used to gain access to the data center **(GRP34)**, and proximity cards are used at data center facilities to restrict access to only authorized personnel **(SOC 2.01)**. Personnel are required to display their identity badges when onsite at Rackspace facilities.

In addition, physical safeguards are in place to restrict access to the server room within the data center **(SOC 2.02)**. Physical access (badge access/biometric access) events are logged and retained for at least 12 months. These logs are available for review in case of an incident or suspicious activity. A Monthly review is conducted to identify unusual patterns. Action is taken to address any patterns discovered. **(GRP36)**. Per the Company's policy, personnel and visitors are required to display their identity badges when onsite at Rackspace data center facilities. Unescorted visitors are not allowed in sensitive areas **(GRP32)**.

Visitors to Rackspace facilities check in with reception/security before being granted access to Rackspace facilities. The visitor log is compiled and retained for 12 months **(SOC 2.03)**.

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.

Appropriateness of physical access to Rackspace data center facilities is reviewed on a periodic basis **(SOC 2.04)**. When physical access is no longer needed due to termination of employment or services, physical access is disabled within the timeframe specified by the User Access Standard **(SOC 2.05)**.

Closed circuit video surveillance has been installed at entrance points on the interior and exterior of the buildings housing data centers and is monitored by authorized Rackspace personnel. The CCTV retention period is at least 90 days **(GRP35)**.

For added security, the data center facilities are not identifiable from the outside of the building or accessible to unauthorized personnel, and security guards are present at the facilities to monitor physical activity and to respond to security incidents **(GRP30)**. In addition, the data centers have an alarm system at exit and entry points to alert security personnel if a door is forced open or left open. Alerts are send to the Physical Security team who document follow-up through the ticketing system **(GRP31)**.

Environmental Controls

Environmental protections, software, and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet availability commitments and requirements. The data center facilities are equipped with redundant HVAC units to maintain consistent temperature and humidity levels **(GRP52)** and to protect against environmental risks. 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)**. The data center facilities are equipped with raised flooring **(GRP60)**.

To prevent and mitigate the risk of loss of data and equipment due to a fire, data center facilities are equipped with fire detection and suppression systems **(GRP61)**, and fire detection systems, sprinkler systems, and chemical fire extinguishers are inspected at least annually **(GRP62)**. To mitigate data loss due to power failures and/or fluctuations, data centers are equipped with uninterruptible power supplies

(UPS) systems **(GRP54)** and diesel generators **(GRP55)**. The UPS systems are inspected and/or serviced at least annually **(GRP63)**, and generators are tested at least every 120 days and serviced at least annually **(GRP64)**.

(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 Data Center Services System.

Operating Systems/Platforms
Rackspace supports a number of different operating systems as part of the Dedicated environment. 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 environment 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 environment.

- 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 environment (e.g. ASA firewalls, Catalyst/Nexus switches, routers).

- eDirectory ("eDir") – This is a suite of identity management tools utilized by Rackspace as the means to control administrative rights for Rackspace systems. eDir is based upon third party software provided by NetIQ and includes the following components:
    - NetIQ Access Governance Suite – components designed to provide reporting and relevant audit-level detail of identity events
    - NetIQ eDirectory – full service, LDAP (lightweight directory access protocol) directory system
    - NetIQ IDM/Vault – Identity management suite with Identity repository (Vault) for NetIQ
    - NetIQ Network Access Manager (NAM) – Web access management tool provides Single-sign on capabilities for web applications
    - NetIQ Sentinel – Real-time monitoring and remediation tool for NetIQ
    - NetIQ SSPR – Self-service password reset tool for Net IQ
    - RackerApp – renamed version of NetIQ's Role-based Provisioning Module, an add-on component of NetIQ Identity Manager to allows role-based provisioning of credentials from eDir

- 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 environment systems.

- 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 for the purposes of PCI DSS compliance.

- 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. The following are relevant components of this 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 Administration – Corporate Environment

Rackspace policies require users to be specifically authorized to access information and system resources. Technology and Engineering Services (TES) is responsible for security administration functions, including the provisioning and deactivation of employee 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 the 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 our customers.

New administrator access to network devices supporting Rackspace infrastructure is granted through the new user creation process. Access is role based and deviations require manager approval **(SOC 5.01)**. The GDCI team maintains a series of examinations that are used to test an employee's technical ability and knowledge of the Rackspace network infrastructure for the purpose of determining the level of access the employee will be granted.

Administrator access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services (Cisco ACS). Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS software **(SOC 5.02)**. User activity is controlled and restricted by defining granular authorization privileges in Cisco ACS. Employees' authorization privileges are based on the examination results administered by the GDCI team as part of the new user creation process. In addition, Cisco ACS access lists are reviewed on a quarterly basis to verify those users on the list still require access to network devices **(SOC 5.03)**.

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.

Rackspace's internal tools and equipment logically reside within the corporate network, thus access to these resources is limited to connections originating from within the network. Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into the network. Although remote network access is permitted, two-factor authentication is required to remotely connect to the Rackspace corporate network **(SOC 5.04)**.

The Global Enterprise Security (GES) Cryptography Policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted **(GRP69)**.

Employee access to the Rackspace corporate network and to customer environments is administered via the Corporate Active Directory and the Intensive Active Directory, respectively. Intensive Active Directory maintains appropriate segregation of duties through the use of various delegation boundaries **(SOC 5.05-D)**. Corporate Active Directory manages all internal infrastructure. Intensive AD manages customer Infrastructure. The two systems do not have access to each other.

Human Resources is the only division authorized to request corporate network accounts for new employees. A request is initiated by adding a job position within the Global People System (GPS) to reflect the hire of a new employee. Nightly, the Corporate Active Directory syncs with the GPS system to determine newly hired employees in need of a network account and searches for terminated employees whose access needs to be removed from the network. By following this process, Rackspace ensures that Human Resources is the authoritative source for the proper granting and removal of employees' logical access to corporate resources. In addition, this process ensures that Corporate Active Directory access is

disabled in a timely manner **(SOC 5.06-D / SOC 5.07-C)** for employees who are no longer with the Company.

When an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts the GET department to modify the transferred emp1oyee's access rights to those that are commensurate with the employee's new position and responsibilities.

Users are assigned a unique ID before allowing them to access system components **(GRP28)**.

Employee access to the corporate 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. The Corporate Active Directory user access list is reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner **(SOC 5.07-D / SOC 5.08-C)**.

Rackspace sends multiple invalid login attempts to the network through the Splunk system **(GRP71)**.

Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system **(SOC 5.08-D / SOC 5.09-C)**. For the Intensive Active Directory, Rackspace has established a minimum password baseline configuration, including parameters over the following **(SOC 6.01-D)**:

- Password history
- Maximum age
- Minimum length
- Complexity

Logical Access Administration – Dedicated Client Environment

Intensive Active Directory passwords used by Rackspace employees are rotated at least every 24 hours **(SOC 6.02-D)**. After an employee has been granted a corporate network account, then an Intensive Active Directory account can be created. New user accounts within the Intensive Active Directory are created based on a person's job function and/or manager approval **(SOC 6.03-D)**.

The Intensive Active Directory user access list is reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner **(SOC 6.04-D)**. An automated process is in place to review each user's current title and group division to ensure access is still appropriate. For users whose title or division is not within a role that supports customer environments, the user's manager approval is required to maintain access for the next three months.

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 read sensitive information regarding customer devices.

Access to hosting environments is administered by allowing connections from a restricted group of computers only **(SOC 6.05-D)**. Rackspace personnel authenticate to a server farm (bastion servers) prior to authentication and connection to a customer device. A bastion server is a gateway and a layer of security positioned between Rackspace infrastructure and the customer infrastructure. It enables the delivery of Rackspace's Fanatical Support 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. Two-factor authentication is used to connect to the bastion servers **(GRP37)**.

Customer environments are isolated from one another via the use of VLAN and separate broadcast domains **(SOC 6.06-D)**. Virtual networks (VLAN) are used to logically segment customers on the

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

Individual Managed Hosting customer configurations utilize dedicated hardware for servers, firewalls, and load-balancers **(SOC 6.07-D)**. In other words, dedicated managed hosting customers are assigned their own hardware and are given full administrative control to this infrastructure. Customer firewalls delineate the boundary between Rackspace shared infrastructure and the customer environment. Rackspace fully manages the administration of shared infrastructure and Rackspace customers retain full administrative rights and control of their environments. The customer is therefore considered the primary system administrator of their environment. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment.

Customers have full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. For customers that selected a firewall, Rackspace makes available the ACL configuration to the customer. **(SOC 6.08-D)**. In addition, Rackspace will communicate the firewall rule set as part of the customer implementation call agenda and it is available for review by the customer via the customer portal.

A firewall rule set can be modified by employees that have been granted an account within the Cisco ACS software, since Cisco ACS administers the access to Rackspace's networking devices. For customer firewalls, modifications to the rule set are also available via the customer portal (MyRackspace™ portal). Only authorized employees have the ability to access the customer firewall manager, which is the module that allows such modifications. Changes to a customer firewall via the MyRackspace™ portal are logged and available for review **(SOC 6.09-D)**. This include changes made by Rackspace employees and changes made by Rackspace customers.

The Rackspace network has several mechanisms and controls in place to safeguard its 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 utilizes data loss prevention software to scan for sensitive information in outgoing transmissions **(GRP39)** to ensure the confidentiality of this type of data.

To reinforce our objective to secure data, the Company's Secure File Transfer and Physical Media Handling Standards define mandatory security measures for when full encryption of removable media is required **(GRP40)**.

Secure connections to Rackspace ticketing systems and the employee HR system is important in order to maintain the confidentiality of the information housed in this system, therefore the customer service platform and Workday are encrypted using strong cryptography protocols such as SSN, VPN or SSL/T S **(GRP24)**.

Incident Management

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. Known vulnerabilities are counter measured by making accessible to customers a Windows and Linux server with the most up to-date patches ready to download and install **(GRP67)**.

In order to trace malicious acts or trace errors in the network, an access control system is used to log administrator activity to network devices. Logged activity includes username, successful/unsuccessful login attempts and timestamp. These logs are retained for one year, and are available for review in case of an incident or suspicious activity **(GRP43)**.

Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.

Incident events are documented in a database that serves as a central repository. Once an event is created, it is assigned a unique identifier, and an e-mail is sent to applicable Rackspace personnel for notification and status update(s) **(SOC 4.03)**. When an incident is resolved, the ticket is closed, documenting the time of the resolution **(SOC 4.04)** to note the time it took to contain the incident and resolve the issue.

A summary of physical and cyber security incidents is compiled and distributed to the Global Security team on a weekly basis to make leadership and appropriate personnel aware of current security challenges and concerns **(GRP48)**.

Change Management

Rackspace has an established Technical Change Management Policy to prevent and reduce service disruptions of Rackspace's shared infrastructure. Service disruptions may occur due to changes such as upgrades, maintenance, 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. Rackspace customers use this shared infrastructure to gain the economies of scale cost advantage benefits that shared infrastructure offers for applicable types of equipment. Examples include core routers, switches. SAN fabric, backup infrastructure, and Internet backbone connections.

Rackspace has instituted a Technical Change Management Policy, which proposed changes to the infrastructure must adhere to. The policy is reviewed on an annual basis **(SOC 3.01)**. Prior to implementation of changes to the production environment, infrastructure changes undergo testing when feasible **(SOC 3.02)**. For this purpose, Rackspace has implemented separate test and production environments for its bastion servers **(GRP51)**. Testing is performed once the Change Sponsor has developed a test plan, relevant technical personnel have vetted this plan, and all necessary equipment is obtained. Typically, testing is performed in a segregated test lab on the Rackspace campus. The level of testing performed is dependent on the nature of the project being implemented and follows the vendor's recommended test strategy, when applicable.

Proposed changes to technical infrastructure are assessed to determine the level of approval and communication required before implementation. Assessment rating consists of the review of the change across three dimensions: impact, likelihood, and redundancy. Technical infrastructure changes with a medium risk rank are escalated to the Change Sponsor for implementation approval **(SOC 3.03)**, and technical infrastructure changes with a high-risk rank are escalated to the Change Sponsor and to the Change Management Board for implementation approval **(SOC 3.04)**.

From change inception to finalization, the Change Board works with relevant stakeholders to validate potential interdependencies have been considered and appropriately addressed.

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

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 our products and services. For findings resulting from risk assessments, a ticket is created to track remediation efforts. **(GRP50)**, and the top five risks resulting from risk assessments are communicated to Security Leadership **(GRP49)**.

Availability

Processing capacity is monitored on a daily basis 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 and Finance **(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.

Redundant lines of communication exist to telecommunication providers **(GRP53)** to protect against availability issues. In addition, fully redundant routing and switching equipment is utilized for Rackspace's core network infrastructure **(GRP56)**. 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 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 tests and updates its business continuity plans regularly 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. A data backup process is in place for customers who have subscribed to the managed backup service. The backup schedule is based on the backup frequency configured in the backup utility software **(SOC 7.01-D)**.

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace has implemented an automated disc failure resolution 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.

Customers subscribed to offsite retention have media sent to an offsite storage facility in a locked container **(SOC 7.02-D)**. Backup tapes are securely destroyed when their useful life expires **(SOC 7.03-D)**.

Rackspace performs weekly monitoring of retention services **(SOC 7.04-D)**.

(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 delineate reporting within each department and job responsibility **(SOC ELC03)**.

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

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

Eight global functions support these segments:

- Engineering
- Accounting & Finance
- Legal
- Employee Services
- 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.

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 all active and approved positions and are effectively utilized (and updated as needed) **(SOX ELC11)**.

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 the best talent to provide fanatical support. Rackspace conducts a security background check/screening in accordance with company policy as well as all local, state, federal, and regional laws **(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 performs 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 achievement of the Company's objectives and strategies **(SOX ELC01)**. Rackspace ensures that personnel have the knowledge and training

needed to perform their duties. New employees go through initial Security training during the New Hire Process **(SOC ELC05)**.

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)**.

(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 Data Center 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 Data Center 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. Responsibility and accountability for the design, development, implementation, communication and maintenance of Rackspace security and availability policies are assigned to and shared amongst different parts of the organization (ISOC, NET SEC, Compliance, Global Enterprise Security teams). **(GRP02)**.

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 expressed 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 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.

Rackspace has defined a risk assessment approach. A Security Risk Management Plan provides a methodology that defines Rackspace's risk assessment approach in identifying, analyzing and evaluating risk, and evaluating options for treatment of risks **(GRP19)**.

A formal Security risk assessment and management process identifies potential threats to the organization. Management identifies and rates risks. Identified risks are rated using a risk evaluation process and ratings per the Security Risk Management Plan **(GRP20)**. The Risk Management team communicates risk mitigation strategies, including the implementation of new controls, to system owners, and risk recommendation items are followed up to note current state or progress **(GRP25)**. Finally, the Risk Management group's recommendations are reviewed and accepted by management **(GRP21)**.

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 aids in identifying potential concerns that would impair system security **(GRP23)**. On an annual basis, Rackspace performs formal risk assessments over its Data Center Services systems **(GRP22)**. Furthermore, on a quarterly basis, the Governance, Risk, and Performance (GRP) team meets with Legal to identify changes that could significantly affect the system of internal control for security and availability **(GRP26)**.

Vendor Management

Rackspace maintains a vendor management program that includes documented policies and standards as follows. These policies and standards are reviewed and approved annually **(SOC ELC06)**:

- Supplier Relationship Management
- Supplier Information Security Risk Management Program
- Supplier Information Security Requirements Standard

Contracts are approved by management at the Vice President level or above or their documented designee. Approval is based on documented and approved signing limits **(SOC ELC07)**.

Finally, 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 and external parties the scope of systems through numerous Compliance documents such as Payment Card Industry (PCI) AOC, ISO 27001 Statement of Applicability, Rackspace Description of Controls, Rackspace Dedicated Frequently Asked Questions (FAOs), and Rackspace Cloud Security 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 ("DC") 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 periodically trained on security expectations **(SOC 1.02)**.

Further support is provided when the Global Enterprise Security team releases periodic communications focusing on immediate security and availability issues and enhancements in security and availability products **(GRP06)**. The Company's commitments and its Information Security Policy are available for review by its employees on the Company Intranet. Reviews are conducted at least annually and updates are performed as needed **(SOC 1.01)**.

Moreover, the Chief Information Security Officer holds a Town Hall meeting at least quarterly with the Global Enterprise Security teams to discuss and communicate the department's goals and expectations **(GRP11)**. 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.

The Hybrid Team creates and communicates to its members a weekly update and status reports on the projects and challenges the division is currently facing and documents it in the Weekly Activity Report (WAR) that is communicated via email. Management, at their discretion, may not send out the WAR due to public holidays or other factors deemed reasonable by management **(GRP12)**. Also, the Rackspace ESWG (Enterprise Security Working Group) meets on a monthly basis to discuss and act on enterprise security concerns. The ESWG group is composed of leaders and representatives from key departments across the Company **(GRP13)**.

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 **(GRP07)**, while the Rackspace Acceptable Use Policy (AUP), also available on the Company website, 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)**.

Security commitment and system operation responsibilities are communicated to third parties through the Master Services Agreement and the Hosted Information Addendum **(GRP70)**.

Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel. Escalation procedures are in place and communicated through the customer portal so the customer can get answers to questions and have increasing levels of authority to which to appeal **(SOC 4.05)**.

Internally, an Incident Response process exists to respond to and document physical and cyber security incidents **(SOC 4.01)**. The Incident Management team provides documented procedures in the IM intranet website, which establishes point of contact(s) and threshold of incident levels **(SOC 4.02)**.

System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner **(SOC 3.05)**.

Internally, technical infrastructure and hardware maintenance changes are scheduled in the ServiceNow (SNOW) calendar tool, 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. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the Change Board.

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.

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.

Rackspace monitors controls to ensure security and availability requirements. Non-conformities found are communicated and resolved with appropriate stakeholders in a timely matter. **(GRP09)**.

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.

The Company undertakes regular reviews of the effectiveness of the Information Security Management System (ISMS) program, taking into account results of security audits, incidents, and results from effectiveness measurements, and suggestions and feedback from all interested parties. For this purpose, Rackspace has established an Information Security Operations Center (ISOC), which is staffed 24 hours a day, 7 days a week, and 52 weeks a year to identify, monitor, and resolve cyber security incidents. On a periodic basis, the ISOC team provides cyber security incident updates to Rackspace leadership **(GRP45)**.

(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.

NOTE: In delivering these services, Rackspace has explicitly communicated to customers that Rackspace is not responsible for encryption of data as part of the Data Center 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 Criteria

Trust Services Principles

This report addresses the following principles as specified by the AICPA Trust Services Principles and Criteria:

- Security – The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.
- Availability – The system is available for operation and use to meet the entity's commitments and system requirements.

Trust Services Criteria and Related Controls

Although the Trust Services Criteria and related controls are presented in Section IV of this report, " Trust Services Principles, Criteria, Rackspace's Related Controls, and PricewaterhouseCooopers LLP's Tests of Operating Effectiveness and Results of Tests ", they are an integral part of Rackspace's description of the Data Center 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. Data Center Services Significant Events

In June 2017 Rackspace went live with a new leased data center FRA1.

On June 20, 2017 Rackspace completed the acquisition of TriCore Solutions. This report does not extend to the controls and processes related to TriCore Solutions.

Except for the two items noted above, there were no other significant changes that occurred to Data Center Services for the period November 1, 2016 to October 31, 2017.

IV. Trust Services Principles, Criteria, Rackspace's Related Controls, and PricewaterhouseCooopers LLP's Tests of Operating Effectiveness and Results of Tests

The AICPA Trust Services Principles, criteria, Rackspace's related controls, and test results are included in this section. For each control 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	**Common Criteria Related to Organization and Management**	
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	SOC ELC03 SOX ELC01 SOX ELC11
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	SOC 1.01 SOC ELC03 SOX ELC11
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.	GRP02 SOC ELC05 SOX ELC01 SOX ELC11
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.	SOC ELC01 SOC ELC02 SOC ELC04
CC2.0	**Common Criteria Related to Communications**	
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	GRP04 SOC 1.01 SOC ELC05
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	GRP04 GRP05 GRP06 GRP07 SOC 1.02
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	GRP02 GRP06 GRP08 GRP70 SOC 1.02 SOC ELC02 SOC ELC05
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	GRP06 GRP10 GRP11 GRP12 GRP13
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	SOC 4.01 SOC 4.02 SOC 4.05

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

Criteria Reference	Criteria Description	Control Reference
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	GRP17 SOC 3.03 SOC 3.04 SOC 3.05
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**	
CC3.1	The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	GRP19 GRP20 GRP21 GRP22 GRP23 GRP26 GRP49 SOC ELC06 SOC ELC07 SOC ELC08
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	GRP09 GRP25 SOC 1.01
CC4.0	**Common Criteria Related to Monitoring of Controls**	
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	GRP09 GRP45
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	GRP71 SOC 5.02 SOC 5.04 SOC 5.05-D SOC 5.08-D / SOC 5.09-C SOC 6.01-D SOC 6.02-D SOC 6.05-D SOC 6.06-D SOC 6.07-D SOC 6.08-D SOC 6.09-D
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	GRP28 SOC 5.01 SOC 5.03 SOC 5.05-D SOC 5.06-D / SOC 5.07-C SOC 5.07-D / SOC 5.08-C SOC 6.03-D SOC 6.04-D SOC 6.08-D

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

Criteria Reference	Criteria Description	Control Reference
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	SOC 5.02 SOC 5.04 SOC 5.08-D / SOC 5.09-C SOC 6.01-D
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	SOC 5.01 SOC 5.03 SOC 5.06-D / SOC 5.07-C SOC 5.07-D / SOC 5.08-C SOC 6.03-D SOC 6.04-D
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	GRP22 GRP30 GRP31 GRP32 GRP34 GRP35 GRP36 SOC 2.01 SOC 2.02 SOC 2.03 SOC 2.04 SOC 2.05 SOC ELC08
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	SOC 5.02 SOC 5.03 SOC 5.04 SOC 5.07-D / SOC 5.08-C SOC 5.08-D / SOC 5.09-C SOC 6.01-D SOC 6.04-D SOC 6.05-D SOC 6.06-D SOC 6.07-D SOC 6.08-D SOC 6.09-D
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	GRP24 GRP37 GRP39 GRP40 GRP41 GRP69
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.	GRP41 SOC 6.07-D SOC 6.08-D SOC 6.09-D
CC6.0	**Common Criteria Related to System Operations**	
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.	GRP36 GRP43 GRP45 GRP47 GRP67 SOC 7.01-D

Criteria Reference	Criteria Description	Control Reference
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	GRP30 GRP45 GRP47 GRP48 SOC 4.01 SOC 4.02 SOC 4.03 SOC 4.04
CC7.0	**Common Criteria Related to Change Management**	
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	SOC 3.01 SOC 3.02 SOC 3.03 SOC 3.04
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	GRP49 GRP50 SOC 3.01 SOC 3.04 SOC 4.01
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	SOC 3.01 SOC 3.04 SOC 4.01
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	GRP51 SOC 3.01 SOC 3.02 SOC 3.03 SOC 3.04
Additional Criteria for Availability		
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	GRP57 GRP58
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	GRP22 GRP52 GRP53 GRP54 GRP55 GRP56 GRP59 GRP60 GRP61 GRP62 GRP63 GRP64 GRP65 SOC 7.01-D SOC 7.02-D SOC 7.03-D SOC 7.04-D SOC ELC08

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

Criteria Reference	Criteria Description	Control Reference
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	GRP65 GRP66

Rackspace Control Activities

The following are the control activities designed and implemented within the Rackspace Data Center Services System to meet the criteria related to the security and availability principles, 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 assigned to and shared amongst different parts of the organization (ISOC, NET SEC, Compliance, Global Enterprise Security teams).	**Inspection** Inspected the Rackspace security and availability policies to determine if the policies are assigned to and shared amongst the ISOC, NET SEC, Compliance, and Global Enterprise Security teams.	No exceptions noted.
GRP04	Rackspace communicates to internal and external parties the scope of systems through numerous Compliance documents: PCI AOC, ISO 27001 Statement of Applicability, Rackspace Description of Controls, Rackspace Dedicated FAQ, and Rackspace Cloud Security FAQ.	**Inspection** Inspected the following Compliance documents to determine if the documents addressed the scope of systems: • PCI AOC • ISO 27001 Statement of Applicability • Rackspace Description of Controls • Rackspace Dedicated FAQ • Rackspace Cloud Security FAQ **Inspection** Inspected evidence to determine if the Compliance documents were made available through the Compliance portal.	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.	**Inspection** Inspected the data center knowledge and community space (DC Wiki) to determine if it was available to Rackers on the Company intranet. **Inspection** Inspected the DC Wiki to determine if the scope and boundaries of the Rackspace Data center systems were documented and if it included policies, procedures, contact personnel and organization structure by region.	No exceptions noted. No exceptions noted.

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

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.	**Inspection** Inspected emails from Global Enterprise Security for a sample of communications to determine if the emails addressed immediate security issues, immediate availability issues, enhancements in security production, and enhancements in availability products.	No exceptions noted.
GRP07	The Rackspace Service Level Agreement (SLA) is communicated via the Company website and includes provisions for network, hardware and infrastructure downtime.	**Inspection** Inspected the Rackspace external website to determine if the Rackspace SLA was available to customers. **Inspection** Inspected the SLA to determine if it included provisions for network, hardware, and infrastructure downtime.	No exceptions noted. 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.	**Inspection** Inspected the Company website to determine if the general terms and conditions were available. **Inspection** Inspected the general terms and conditions to determine if Rackspace's commitment regarding the system's security and availability was included.	No exceptions noted. No exceptions noted.
GRP09	Rackspace monitors controls to ensure security and availability requirements are met. Non-conformities found are communicated and resolved with appropriate stakeholders in a timely matter.	**Inspection** Inspected the annual Internal Audit Compliance Schedule and Nonconformities tracking documents to determine if Rackspace monitored controls. **Inspection** Inspected the annual Internal Audit Compliance Schedule and Nonconformities tracking documents to determine if nonconformities were communicated and resolved.	No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
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.	**Inspection** Inspected the Acceptable Use Policy (AUP) to determine if the document specified activities not allowed by customers. **Inspection** Inspected that the AUP was available on the Company website.	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 from the UK and the US to discuss and communicate the department's goals and expectations.	**Inspection** Inspected the invite emails and agendas associated with each Town Hall meeting for a sample of meetings and determine if attendees included members of the Global Enterprise Security teams and included communication regarding the department's goals and expectations.	No exceptions noted.
GRP12	The Rackspace Hybrid team creates and communicates the WAR (Weekly Activity Report). The report is updated weekly with status reports from the Hybrid division. Management at their discretion may not send out the weekly WAR due to public holidays or other factors deemed reasonable.	**Inspection** Inspected emails associated with the Weekly Activity Reports for a sample of weeks and determined if the reports were disseminated via email and included status reports from the Hybrid division.	No exceptions noted.
GRP13	The Rackspace ESWG (Enterprise Security Working Group) meets on a monthly basis to discuss and act on enterprise security concerns. The ESWG group is composed of leaders and representatives from key departments across the Company.	**Inspection** Inspected emails, agendas and meeting notes associated with the ESWG meeting for a sample of months and determined if the group is (1) composed of representatives from across the Company, and (2) the group discussed and acted on enterprise security concerns.	No exceptions noted.
GRP17	Change requests are displayed on the ServiceNow (SNOW) maintenance calendar, which is visible to Rackspace employees.	**Inspection** Inspected evidence to determine if 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.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
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.	**Inspection** Inspected the Security Risk Management Plan to determine if 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	Identified risks are rated using a risk evaluation process and ratings per the Security Risk Management Plan.	**Inspection** Inspected the risk assessment documentation for a sample of risk assessments and determined if the risks were evaluated and rated in accordance with the Security Risk Management Plan.	No exceptions noted.
GRP21	The Risk Management Group's recommendations are reviewed and accepted by management.	**Inspection** Inspected the risk assessment documentation for a sample of risk assessments and determined if the assessments were signed by management of the respective area to signify review and acceptance of the risk management group's recommendations.	No exceptions noted.
GRP22	On an annual basis, Rackspace performs formal risk assessments over its Data Center services systems.	**Inspection** Inspected the risk assessment documentation for a sample of risk assessments to determine if the annual risk assessments were conducted related to the Data Center Services systems.	No exceptions noted.
GRP23	A Threat and Vulnerability Analysis team exists to identify any potential concerns that would impair system security.	**Inspection** Inspected the Vulnerability Management Standard to determine if the policy included steps for identifying potential concerns that would impair system security. **Inspection** Inspected an organizational chart of the Threat and Vulnerability Team to determine if the team was organized and structured to identify any potential concerns that would impair system security.	No exceptions noted. No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP24	Access to Rackspace's customer service platform and Workday are encrypted using strong cryptography protocols such as SSN, VPN or SSL/TLS.	**Inspection** Inspected the customer service platform and Workday to determine if cryptography protocols such as SSN, VPN or SSL/TLS are in place.	No exceptions noted.
GRP25	The Risk Management team communicates risk mitigation strategies, including the implementation of new controls, to system owners. Risk recommendation items are followed up to note current state or progress.	**Inspection** Inspected evidence that the risks were tracked and followed up to resolution within the risk assessment or a ticket for a sample of risks from conducted risk assessments.	No exceptions noted.
GRP26	On a quarterly basis the Governance, Risk, and Performance (GRP) team meets with Legal to identify any changes that could significantly affect the system of internal controls for security and availability.	**Inspection** Inspected meeting invites, meeting minutes and agendas for a sample of meetings to determine if the GRP and Legal teams met to identify changes that could significantly affect the system of internal controls for security and availability.	No exceptions noted.
GRP28	Users are assigned a unique ID before allowing them to access system components.	**Inspection** Inspected evidence that a duplicate account could not be created within Cisco ACS.	No exceptions noted.
GRP30	Security guards are present at Rackspace data center facilities to monitor physical activity and to respond to security incidents.	**Observation** Observed security guards were present at each in-scope data center to monitor physical activity and to respond to security incidents.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP31	Rackspace data center facilities have an alarm system at exit and entry points to alert security personnel if a door is forced open or left open. Alerts are delivered to the Physical Security Team who follow up and document actions taken.	**Observation** Observed an alarm system was in place at entry and exit points of each in-scope data center. **Observation** Observed the alert triggered upon attempt to prop open a door to an in-scope data center. **Observation** Observed the security system console at each in-scope data center to determine the system was available to manage the alarm system. **Observation** Observed the Physical Security Team determine and document process of follow-up and documentation through the alarm monitoring system. **Inspection** Inspected an example of follow-up/resolution documentation.	No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted. No exceptions noted.
GRP32	Visitors at Rackspace facilities must check in with reception/security before being granted access to Rackspace facilities. Personnel and visitors are required to display their identity badges when onsite at Rackspace data center facilities. Unescorted visitors are not allowed in sensitive areas.	**Observation** Observed that personnel and visitors must check in with reception/security before being granted access. **Observation** Observed personnel and visitors display identity badges when onsite at in-scope Rackspace data center facilities.	No exceptions noted. No exceptions noted.
GRP34	Two factor authentication is used to gain access to the data center.	**Observation** Observed two factor authentication was required to gain access to each in-scope data center.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP35	Closed circuit video surveillance is monitored by authorized personnel 24x7. CCTV retention period is at least 90 days for data centers.	**Observation** Observed cameras installed to verify entrance points on the interior and exterior of each in-scope data center building. **Observation** Observed the video feed from 90 days prior to ensure CCTV media was retained for 90 days.	No exceptions noted. No exceptions noted.
GRP36	Physical access (badge access/biometric access) events are logged and monitored real time and alerts are generated and acted upon as appropriate. A Monthly review is conducted to identify unusual patterns. Action is taken to address any patterns discovered.	**Observation** Observed physical access events are logged and monitored real time. **Observation** Observed someone use their badge and traced event to logging. **Inspection** Inspected the review conducted to identify unusual patterns for a sample of months to verify appropriate action was taken to address any patterns discovered.	No exceptions noted. No exceptions noted. No exceptions noted.
GRP37	Two factor authentication is used to connect to the bastion servers.	**Observation** Observed an attempt to connect to a bastion server without two factor authentication and determine if the connection was unsuccessful. **Observation** Observed an attempt to connect to a bastion server with two factor authentication and determine if the connection was successful. **Inspection** Inspected the associated bastion configuration and determine if two factor authentication is required to access the bastion servers.	No exceptions noted. No exceptions noted. No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP39	The Rackspace team utilizes a data loss prevention software to scan for sensitive information in outgoing transmissions.	**Inspection** Inspected the Websense policy listing to determine if data loss prevention software was in place and configured to scan for sensitive information in outgoing transmissions. **Inspection** Inspected an example email alert to determine if data loss prevention software alerts upon detecting sensitive information in outgoing transmissions.	No exceptions noted. 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.	**Inspection** Inspected the Secure File Transfer Standard and the Physical Media Handling Standard to determine if the standards outline 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.	**Inspection** Inspected a network diagram and determine if an IDS was implemented on the Rackspace network. **Inspection** Inspected an example alert and determine 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.	**Observation** Observed a failed login attempt to determine if the activity was logged. **Observation** Observed archived logs to determine if logs are retained for at least one year.	No exceptions noted. No exceptions noted.
GRP45	On a periodic basis the ISOC team provides cyber security incident updates to Rackspace leadership.	**Inspection** Inspected evidence for a sample of high and critical severity cybersecurity incidents that an incident update was shared with Rackspace leadership.	No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP47	Rackspace has implemented an automated disc failure resolution process in order to mitigate the risk of faulty media.	**Inspection** Inspected the SmartFail configuration to determine if the tool was configured to automatically alert upon media failures. **Observation** Observed the automated detection of an example media failure to determine if SmartFail detected and remediated faulty media.	No exceptions noted. No exceptions noted.
GRP48	Rackspace security events are reported and distributed to the appropriate global security team members on a weekly basis.	**Inspection** Inspected that security events are consolidated and reported for a sample of weeks.	No exceptions noted.
GRP49	The Risk Management team communicates the top five risks resulting from risk assessments to Security Leadership.	**Inspection** Inspected the annual Enterprise Risk Management meeting invitation and Top Risks presentations and determine if the Risk Management team communicated the top five risks resulting from risk assessments to Security Leadership.	No exceptions noted.
GRP50	For findings resulting from risk assessments a ticket is created to track remediation efforts.	**Inspection** Inspected the corresponding risk documentation for a sample of risks from conducted risk assessments to determine a ticket was created to track remediation efforts.	No exceptions noted.
GRP51	Rackspace has implemented separate test and production environments for its bastion servers.	**Inspection** Inspected evidence to determine if there are separate test and production environments for bastion servers.	No exceptions noted.
GRP52	The data center facilities are equipped with redundant HVAC units to maintain consistent temperature and humidity levels.	**Observation** Observed HVAC units are present at each in-scope data center. **Observation** Observed the capacity load of each HVAC unit to determine there are redundant HVAC units.	No exceptions noted. No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
GRP53	Redundant lines of communication exist to telecommunication providers.	**Observation** Observed telecommunication lines are present at each in-scope data center. **Inspection** Inspected the network diagram for each in-scope data center, and determined if redundant lines of communication exist to telecommunication providers.	No exceptions noted. No exceptions noted.
GRP54	Data center facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short term utility power failures and fluctuations.	**Observation** Observed each in-scope data center was equipped with an uninterruptible power supply (UPS).	No exceptions noted.
GRP55	Data center facilities are equipped with diesel generators to mitigate the risk of long term utility power failures and fluctuations.	**Observation** Observed each in-scope data center was equipped with diesel generators to mitigate the risk of long term utility power failures and fluctuations.	No exceptions noted.
GRP56	Rackspace utilizes fully redundant routing and switching equipment for its core network infrastructure.	**Observation** Observed the use of routers for each in-scope data center and determined if Rackspace utilizes fully redundant routing and switching equipment for its core network infrastructure.	No exceptions noted.
GRP57	Processing capacity is monitored on a daily basis by data center personnel via the Data Center Operations Metrics dashboard.	**Inspection** Inspected the Data Center Operations Metrics dashboard and determine if the dashboard included details related to processing capacity at each data center.	No exceptions noted.
GRP58	Data center capacity utilization is reviewed on a monthly basis by DC Leadership and Finance.	**Inspection** Inspected the communications for a sample of months to determine that data center capacity utilization was reviewed, an attached report was sent to data center leadership, and that the communication contained information regarding power utilization for each data center.	No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
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.	**Observation** Observed smoke detectors at each in-scope data center. **Observation** Observed floor water detectors where chilled water systems were used as coolant at each in-scope data center. **Observation** Observed other environmental hazard sensors (e.g. humidity or temperature sensors).	No exceptions noted. No exceptions noted. No exceptions noted.
GRP60	The data center facilities are equipped with raised flooring.	**Observation** Observed each in-scope data center was equipped for raised flooring.	No exceptions noted.
GRP61	Data center facilities are equipped with fire detection and suppression systems.	**Observation** Observed fire detection and suppression systems were in-place at each in-scope data center.	No exceptions noted.
GRP62	Fire detection systems, sprinkler systems, and chemical fire extinguishers are inspected at least annually.	**Inspection** Inspected evidence that fire detection systems, sprinkler systems, and chemical fire extinguishers were inspected within the past year.	No exceptions noted.
GRP63	The UPS systems are inspected and/or serviced at least annually.	**Inspection** Inspected evidence that the UPS system at each in-scope data center was inspected/serviced within the past year.	No exceptions noted.
GRP64	Generators are tested at least every 120 days and serviced at least annually.	**Inspection** Inspected evidence that the diesel generator at each in-scope data center has been tested within the past 120 days. **Inspection** Inspected evidence that the diesel generator at each in-scope data center has been serviced within the past year.	No exceptions noted. No exceptions noted.

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

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.	**Inspection** Inspected evidence to determine if a Data Center business continuity plan (BCP) existed 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 tests and updates regularly its business continuity plans to confirm that they are up to date and effective.	**Inspection** Inspected the business continuity plan testing log from the Rackspace GDCI wiki to determine if business continuity plans were tested annually to confirm that they are up to date and effective.	No exceptions noted.
GRP67	Windows and Linux management server (repository) tools are used to make patches available to customers.	**Inspection** Inspected configuration of the Windows patch management server to determine if the server, used to manage Windows patches, was set to synchronize daily. **Inspection** Inspected the Cron job used to schedule updates to the Red Hat Network Satellite, used to manage Linux patches, to determine if it was set to synchronize daily.	No exceptions noted. 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.	**Inspection** Inspected the GES Cryptography Policy to determine if 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 security commitments and system operation responsibilities to third parties through the Master Services Agreement and the Hosted Information Addendum.	**Inspection** Inspected the Master Services Agreement and the Hosted Information Addendum to determine if the documents communicated security commitments and system operation responsibilities to third parties.	No exceptions noted.
GRP71	Rackspace sends multiple invalid login attempts to the network through the Splunk system.	**Inspection** Inspected evidence to determine if failed login attempts to the network were logged within Splunk.	No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
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.	**Inspection** Inspected the Information Security Policy to determine that it was in place and available to personnel on the company intranet. **Inspection** Inspected evidence to determine if 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 periodically trained on security expectations.	**Inspection** Inspected evidence that a Security Awareness Policy existed. **Inspection** Inspected evidence to determine if the workforce was trained at least annually on security expectations.	No exceptions noted. No exceptions noted.
SOC 2.01	Proximity cards are used at Rackspace data center facilities to restrict access to only authorized personnel.	**Observation** Observed an attempt to gain access to each in-scope data center without a proximity card. **Observation** Observed an authorized employee access the data center with proximity card.	No exceptions noted. No exceptions noted.
SOC 2.02	Physical safeguards are in place to restrict access to the server room within the data center.	**Observation** Observed the presence of physical safeguards outside the server room for each in-scope data center to determine if access was appropriately restricted. **Observation** Observed an invalid attempt to gain access to server room to determine that access was appropriately restricted to individuals with a badge. **Observation** Observed a valid attempt by authorized individual to gain access to server room to determine that access was appropriately restricted to individuals with a badge.	No exceptions noted. No exceptions noted. No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 2.03	The visitor log is compiled and retained for 12 months. The log is reviewed in the case of incident or emergency situations.	**Inspection** Inspected the visitor logs for the in-scope data centers to validate that they were retained for 12 months.	No exceptions noted.
SOC 2.04	Appropriateness of physical access to Rackspace data center facilities is reviewed on a periodic basis.	**Inspection** Inspected evidence for a sample of monthly physical access reviews to determine if the reviews were performed and follow-up actions were completed.	No exceptions noted.
SOC 2.05	Physical access is disabled within the timeframe specified by the User Access Standard.	**Inspection** Inspected badge history within the badge access system for a sample of terminated employees and determined if access was disabled within the timeframe specified by the User Access Standard.	No exceptions noted.
SOC 3.01	Rackspace has instituted a Technical Change Management Policy which proposed changes to the infrastructure must adhere to. The Technical Change Management Policy is reviewed on an annual basis.	**Inspection** Inspected evidence to determine if the Technical Change Management Policy was reviewed annually.	No exceptions noted.
SOC 3.02	Infrastructure changes undergo testing when technically feasible.	**Inspection** Inspected evidence for a sample of changes that testing was performed when technically feasible.	No exceptions noted.
SOC 3.03	Technical infrastructure changes with a medium risk rank are escalated to the Change Sponsor for implementation approval.	**Inspection** Inspected evidence for a sample of technical medium risk rank infrastructure changes that the Change Sponsor approved the change prior to implementation.	No exceptions noted.
SOC 3.04	Technical infrastructure changes with a high risk rank are escalated to the Change Sponsor and to the Change Management Board for implementation approval.	**Inspection** Inspected evidence for a sample of technical high risk rank infrastructure changes that the Change Sponsor and the Change Management Board approved the change prior to implementation.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 3.05	Rackspace customers are notified of changes as follows: * At least 72-hours for Dedicated customer changes. *At least 72-hours for Cloud disruptive changes. * Up to 72-hours for scheduled emergency changes.	**Inspection** Inspected evidence for a sample of changes that changes were communicated to customers prior to the change implementation in line with the schedule defined for that type of change.	No exceptions noted.
SOC 4.01	An Incident Response process exists to respond to and document physical and cyber security incidents.	**Inspection** Inspected that the incident management process was followed for a sample of incident tickets.	No exceptions noted.
SOC 4.02	Incident Management procedures are available in the IM intranet website to establish point(s) of contact and threshold of incident levels.	**Inspection** Inspected the Incident Management procedures to determine if they established points of contact and thresholds of incident levels.	No exceptions noted.
SOC 4.03	Once an incident management event is created a communication email is sent to applicable Rackspace personnel for notification and status update(s).	**Inspection** Inspected evidence that a communication email was sent to applicable Rackspace personnel for notification and status update(s) for a sample of incident tickets.	No exceptions noted.
SOC 4.04	When an incident is resolved, the ticket is closed documenting the time of the resolution.	**Inspection** Inspected evidence that the resolution was documented for a sample of incident tickets.	No exceptions noted.
SOC 4.05	Escalation procedures are in place and communicated through the customer portal so the customer can get answers to questions and have increasing levels of authority to which to appeal.	**Inspection** Inspected evidence for a sample of customers that escalation procedures were in place and were communicated through the customer portal.	No exceptions noted.
SOC 5.01	New administrator access to network devices supporting Rackspace infrastructure is granted through the new user creation process. Access is role based and deviations require manager approval.	**Inspection** Inspected that access was appropriate for a sample of new administrators based on role responsibilities and any deviations were approved by a manager.	No exceptions noted.
SOC 5.02	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS software.	**Inspection** Inspected the firewall configuration for a sample of customer firewalls to determine inherent access control functionality in Cisco ACS software was utilized.	No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 5.03	Cisco ACS access lists are reviewed on a quarterly basis to verify those users on the list still require access to network devices.	**Inspection** Inspected the Cisco ACS access lists for all four quarters to determine that they were reviewed timely and any users flagged for access modification were remediated timely.	No exceptions noted.
SOC 5.04	Two factor authentication is used to remotely connect to the Rackspace Corporate Network.	**Observation** Observed a Rackspace employee unsuccessfully connect to the Rackspace Corporate Network without utilizing two factor authentication. **Observation** Observed a Rackspace employee successfully connect to the Rackspace Corporate Network utilizing two factor authentication. **Inspection** Inspected the configuration that required users to authenticate through a VPN.	No exceptions noted. No exceptions noted. No exceptions noted.
SOC 5.05-D	Active Directory maintains appropriate segregation of duties through the use of various delegation boundaries.	**Inspection** Inspected evidence for a sample of customers the customer organizational unit (OU) within Intensive Active Directory was segregated from other customers.	No exceptions noted.
SOC 5.06-D / SOC 5.07-C	Corporate Active Directory access is disabled in a timely manner.	**Inspection** Inspected evidence for a sample of terminated employees that the user's access was disabled timely.	No exceptions noted.
SOC 5.07-D / SOC 5.08-C	The Corporate Active Directory user access list is reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner.	**Inspection** Inspected the Corporate Active Directory user access review for a sample of quarters to determine that the review was performed by an appropriate reviewer, the user list reviewed is complete and accurate, and any discrepancies were corrected timely.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 5.08-D / SOC 5.09-C	Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system.	**Inspection** Inspected the Default Domain Policy and compared it to Rackspace's Authentication Standard to determine if Rackspace established a minimum password baseline configuration for its Corporate Active Directory system.	No exceptions noted.
SOC 6.01-D	Rackspace has established a minimum password baseline configuration for its Intensive Active Directory system, including the following parameters: • Password history • Maximum age • Minimum length • Complexity	**Inspection** Inspected the password configuration settings for Intensive Active Directory to determine if a minimum password baseline was configured, including the following parameters: • Password history • Maximum age • Minimum length • Complexity	No exceptions noted.
SOC 6.02-D	Intensive Active Directory passwords used by Rackspace employees are rotated at least every 24 hours.	**Observation** Observed a Rackspace employee check out an Intensive Active Directory account and observed that the account was set to expire after 24 hours. **Observation** Observed the account expire and determined that the user can no longer access the account.	No exceptions noted. No exceptions noted.
SOC 6.03-D	New user accounts within Intensive Active Directory are created based on job function and/or manager approval.	**Inspection** Inspected evidence for a sample of new user accounts within Intensive Active Directory to determine if new accounts were created with manager approval.	No exceptions noted.
SOC 6.04-D	The Intensive Active Directory user access list is reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner.	**Inspection** Inspected evidence for a sample of quarters that the Intensive Active Directory user list was reviewed by appropriate personnel, completely and accurately, and any modifications of access required were remediated timely.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 6.05-D	Access to hosting environments is administered by allowing connections from a restricted group of computers only.	**Inspection** Inspected the firewall configuration for a sample of customer firewalls to determine access was administered by allowing connections from bastion servers only.	No exceptions noted.
SOC 6.06-D	Customer environments are isolated from one another via the use of VLAN to separate broadcast domains.	**Inspection** Inspected evidence for a sample of customers that the VLANs associated with each customer's switch(es) were segregated.	No exceptions noted.
SOC 6.07-D	Individual Managed Hosting customer configurations utilize dedicated hardware for servers, firewalls, and load-balancers.	**Inspection** Inspected the corresponding CORE ticket for a sample of customers to determine customers had dedicated devices.	No exceptions noted.
SOC 6.08-D	For customers that selected a firewall, Rackspace makes available the ACL configuration to the customer.	**Inspection** Inspected evidence for a sample of customer firewalls that Rackspace made the ACL configuration available to the customer.	No exceptions noted.
SOC 6.09-D	Changes to a customer firewall via the MyRackspace™ portal are automatically logged and available for review.	**Inspection** Inspected evidence to determine if a change to a customer firewall via the MyRackspace™ portal is logged in a change ticket and the SPLUNK tool, and was available for review.	No exceptions noted.
SOC 7.01-D	Backups are scheduled and performed for customers who have subscribed to the managed backup service based on the backup frequency configured in the backup utility software.	**Inspection** Inspected evidence for a sample of devices that the managed backup service was configured in accordance with the customer's subscribed frequency.	No exceptions noted.
SOC 7.02-D	Customers subscribed to offsite retention have media sent to an offsite storage facility in a locked container.	**Observation** Observed each tape selected for a sample of tapes was on-site at the data center. **Observation** Observed each tape selected for a sample of tapes on-site was locked in a secured container.	No exceptions noted. No exceptions noted.

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

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC 7.03-D	Backup tapes are securely destroyed when their useful life expires.	**Inspection** Inspected evidence for a sample of expired tapes that the tape was securely destroyed.	No exceptions noted.
SOC 7.04-D	Rackspace performs weekly monitoring of retention services.	**Inspection** Inspected evidence for a sample of weeks that weekly monitoring of retention services was performed.	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.	**Inspection** Inspected the Rackspace employee handbook and determine the following topics are 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. **Inspection** Inspected evidence for a sample of new hires that each user 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.	**Inspection** Inspected the annual Code of Conduct and Ethics testing results from the Learning Management System (LMS) and determined that 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.	**Inspection** Inspected the Organizational Directory and determined that the organization structure was maintained, including 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.	**Inspection** Inspected the background checks performed for a sample of new hires and determined that employees were subjected to the appropriate background check during the hire process.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOC ELC05	New Employees go through initial Security training during the New Hire Process.	**Observation** Observed the initial Security training performed as part of the New Hire process. **Inspection** Inspected the onboarding sign-in sheet for a sample of new hires and determined the new hires attended the initial Security training.	No exceptions noted. No exceptions noted.
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.	**Inspection** Inspected evidence to determine if the Supplier Relationship Management Policy, the Supplier Information Security Risk Management Program, and the Supplier Information Security Requirements Standard were reviewed and approved within the past year.	No exceptions noted.
SOC ELC07	Contracts are approved by a VP or above (or designee) based on approved signing limits. If the contract consists of a primary agreement and supporting schedules, the scope of the control is limited to the primary agreement.	**Inspection** Inspected the primary agreement for a sample of contracts to determine if each contract was approved by a VP or above (or designee).	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.	**Inspection** Inspected evidence for each leased data center that Rackspace has reviewed third party assurance reports or performed an annual Physical Security and Environmental on-site audit within the past year.	No exceptions noted.
SOX ELC01	At least annually, the Human Resources Team/Management performs 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.	**Inspection** Inspected evidence to determine if key talent was reviewed annually.	No exceptions noted.

Control Reference	Control Activity	PricewaterhouseCoopers' Test Procedure(s)	Results of Test(s)
SOX ELC11	Formal job descriptions exist for all active and approved positions and are effectively utilized (and updated as needed).	**Inspection** Inspected that a formal job description were documented, included required job qualifications, and, if needed, were updated for a sample of active positions.	No exceptions noted.

(This page has been intentionally left blank.)