



RACKSPACE US, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

DATA CENTER HOSTING SERVICES SYSTEM

FOR THE PERIOD OF OCTOBER 1, 2023, TO SEPTEMBER 30, 2024

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Rackspace US, Inc.:

We have examined Rackspace US, Inc.'s ("Rackspace") accompanying assertion titled "Assertion of Rackspace US, Inc. Service Organization Management" ("assertion") that the controls within Rackspace's data center hosting services system ("system") were effective throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Rackspace uses various subservice organizations for data center hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Rackspace, to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Rackspace is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved. Rackspace has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Rackspace is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

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

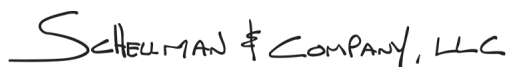
Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Rackspace's data center hosting services system were effective throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHEELMAN & COMPANY, LLC

Columbus, Ohio
November 1, 2024

ASSERTION OF RACKSPACE US, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Rackspace's data center hosting services system ("system") throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Rackspace's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Rackspace's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2023, to September 30, 2024, to provide reasonable assurance that Rackspace's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE DATA CENTER HOSTING SERVICES SYSTEM

Company Background

Rackspace Technology, Inc (“Rackspace”) began operations in December 1993 to provide managed web hosting services to businesses on tools including Amazon Web Services (AWS), Google, VMware, Microsoft, OpenStack®, and others. Today, Rackspace serves over 300,000 customers in 33 data centers worldwide. Currently, Rackspace employs over 6,500 people (Rackers) around the world. Rackspace integrates industry leading technologies and practices for each customer's specific need and delivers it as a service via the company's commitment to Fanatical Experience®.

Description of Services Provided

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

Data center hosting services offerings come in the following forms:

- Dedicated servers for high-performance workloads
- VMware managed environments
- Multi-cloud connectivity with scalability via third-party cloud services
- Database management
- Dedicated directly attached storage (DAS), storage area network (SAN), backup and network attached storage (NAS)
- Secure network infrastructure management

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

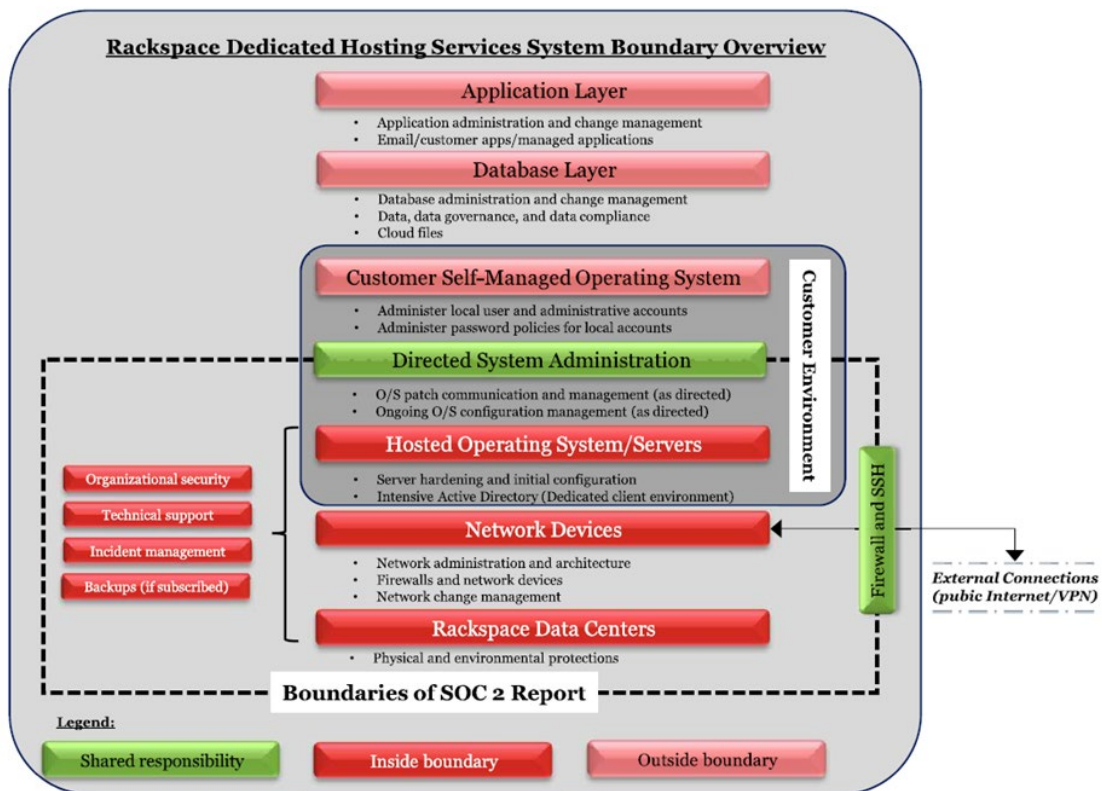
This report covers the data center hosting services system at the following data centers (in-scope data centers):

Physical Location			
Data Center	Location	Ownership Type	Vendor
DFW3	Richardson, Texas	Leased	Digital Realty
FRA1	Frankfurt, Germany		Equinix
FRA2	Frankfurt, Germany		
HKG5	Hong Kong, China		Digital Realty
IAD3	Ashburn, Virginia	Leased	Digital Realty

Physical Location			
Data Center	Location	Ownership Type	Vendor
LON3	Slough, United Kingdom	Owned/Operated	Rackspace
LON5	Crawley, United Kingdom	Leased	Digital Realty
MCI1	Kansas City, Missouri	Owned/Operated	Rackspace
NYC2	Somerset, New Jersey		
ORD1	Elk Grove Village, Illinois	Leased	Digital Realty
SHA3	Shanghai, China		Shanghai Data Solution Co. Ltd.
SIN3	Singapore		Iron Mountain
SJC3	San Jose, California		Digital Realty
SYD2	Sydney, Australia		
SYD4	Sydney, Australia		Equinix

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

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



Principal Service Commitments and System Requirements

Rackspace designs its processes and procedures to meet its objectives for the data center hosting services system. Those objectives are based on the service commitments that Rackspace makes to its customers. Security and availability commitments to customers are documented and communicated in the data center hosting services product terms and standardized contracts.

Security and availability commitments are standardized and include, but are not limited to, the following:

Principal Service Commitments and System Requirements		
Trust Services Category	Service Commitments	System Requirements
Security	<ul style="list-style-type: none">• System access is granted to authorized individuals• System administrators must complete annual security awareness training• Centralized logging and monitoring• Secure configuration management of infrastructure and servers• Preventative system maintenance and patch management• Identification and remediation of risks and vulnerabilities• Data center security controls to prevent unauthorized access to systems• Network security and network access management• Monthly vulnerability scanning of client environments• Endpoint security management for client virtual servers• Security Incident Response (IR) event detection, investigation, and response	<ul style="list-style-type: none">• Identity, access, and personnel management standards and processes• Security awareness and training standards• Audit and accountability standards and processes• Secure configuration standards and configuration management processes• System maintenance and patch management processes• Physical access and environmental standards• System and communication controls and standards• Vulnerability management standards and processes• Centralized endpoint security management platform and standards• IR Plan and processes• Encryption standards• Change management procedures
Availability	<ul style="list-style-type: none">• Systems are available for operation and use and monitored as committed or agreed• Ability to backup and restore systems• Disaster recovery services	<ul style="list-style-type: none">• Monitoring and alerting standards and processes• Backup and recovery processes• Primary and disaster recovery architecture• Disaster recovery planning and testing processes• Physical and environmental standards

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

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

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

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

Rackspace supports a large number of network devices that operate to support the data center hosting services system. Network devices within the system boundaries include:

- Brocade switches
- Cisco Adaptive Security Appliance (ASA) firewalls
- F5 Networks Big-internet protocol (IP) firewalls
- Cisco routers
- Cisco Catalyst switches and Cisco Nexus switches

In supporting both the data center hosting services system as well as providing support to Rackspace customers, Rackspace has implemented a series of tools that support authentication and authorization of individuals. Technologies within the system boundaries include:

- Active Directory (AD) – Rackspace utilizes Microsoft AD to provide identity management via directory services for Rackspace employees as well as managing Microsoft server operating systems in the data center hosting services system.
- Active Directory Federation Services (ADFS) – standards-based service that allows the secure sharing of identity information between trusted business partners (federations) across an extranet.
- Cisco Access Control Server (ACS) – Cisco ACS 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 data center hosting services system (e.g., ASA firewalls, Catalyst/Nexus switches, routers).
- SailPoint IdentityIQ (IIQ) – governance-based identity access management (IAM) solution that provides automated access certifications, policy management, access request and provisioning, password management, and identity intelligence.
- Rivest, Shamir, Adelman (RSA) – RSA authentication manager is utilized as the means to provide tokens with rolling personal identification numbers (PIN) codes to enable multi-factor authentication 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.
- Password Safe – a password management system that is used to securely store, organize, and manage privileged account information and passwords.

Other Tools and / or Services Supporting Infrastructure Components

Rackspace provides tools and services for customers based upon their request and direction. Some of these 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).
- CrowdStrike Falcon Intel - provides next-generation antivirus, endpoint detection and response, and cyber threat intelligence.
- Trend Micro Cloud One - Workload Security (TRND) - SaaS based file Integrity monitoring (FIM) and log inspection platform.
- Intrusion Detection System (IDS) - 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 - security information and event management (SIEM) system that provides real-time visibility across the information security systems and alerts Rackspace employees based on predefined event triggers.
- 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).
- 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 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 storage media.
- Rackspace Virtual Infrastructure - includes the management components of the virtualized infrastructure hosting service. This environment uses the VMware 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 remote desktop protocol (RDP) or secure shell (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 access control lists on the ServiceNet switches also enforce separation of this network.

The in-scope infrastructure consists of multiple systems and platforms, as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
AD	Directory Service used to manage user accounts, access, and authentication requirements to the in-scope systems.	Windows	Refer to Physical Location Table

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Production Servers	Architecture that supports the data center hosting services system.	CentOS Red Hat Enterprise Linux Ubuntu Linux Windows Server O/S	Refer to Physical Location Table
Bastion Host	Provide application layer filtering and proxying of connections into in-scope environments.	Balabit Shell Control Box	
Virtual Private Network (VPN)	Provides secure tunnel for remote connection to hosted environment.	AppGate Global Protect	
Virtualization	Hypervisor and virtual host management.	VMWare vSphere	

People

Personnel involved in the operation and use of the system are:

- The Rackspace leadership team – actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
- The board of directors – consists of members independent from management and has established subcommittees to provide oversight and monitoring of key risk areas (e.g., audit committee, compensation committee, and compliance committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- IT personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure.

Procedures

Access Requests and Access Revocation to the Corporate Network Infrastructure and Customer Environments

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

The global data center infrastructure (GDCI) team administers access to network infrastructure. Network infrastructure is categorized in two sets, Rackspace's network infrastructure (shared infrastructure) and customer's network infrastructure. The GDCI team manages Rackspace's network infrastructure, whereas the network security (NetSec) team manages the customer's network infrastructure.

New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval. Human Resources is the only division authorized to request corporate network accounts for new employees. The request is initiated by adding a job position within the global people system (GPS) to reflect

the hire of a new employee. The corporate AD synchronizes with the GPS system on a nightly basis to determine newly hired employees in need of a network account. Upon receiving AD credentials, the new employee's manager is responsible for initiating an access request for any elevated or administrative access. Users request access to elevated or administrative rights through the SailPoint tool, which are then reviewed and approved / rejected. Following approval through SailPoint, an automated workflow will add users to the approved group, thereby allowing access. User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.

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

Access, Authentication and Authorization to the Corporate Infrastructure

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

Rackspace has established a minimum password baseline configuration for its corporate AD and production server operating systems that is compliant with the Rackspace authentication standard to further restrict access to the production environment.

Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into each network. Access to the Rackspace network is restricted to authorized personnel only. A VPN is restricted to authorized employees with a valid multi-factor authentication (MFA) token over an encrypted VPN connection.

Administrative access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services. Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS. User activity is controlled and restricted by defining granular authorization privileges based on corporate AD groups. User access privileges to in-scope production environments are reviewed on a quarterly basis to help ensure that access to in-scope systems is authorized. Within the quarterly review, users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed.

Access, Authentication and Authorization to Customer Environments

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

Access to hosting environments is restricted by only allowing connections from bastion servers through the use of firewall rules. Bastion servers operate as gateways, logging devices, and provide a layer of security between Rackspace infrastructure and the customer infrastructure; bastion servers enable the delivery of Rackspace services while logging protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific AD access group. Bastions provide security to customer environments by restricting access, ensuring the Rackspace infrastructure interfacing with the customer environment is secure. Rackspace personnel authenticate to a bastion server prior to authentication and connection to customer devices. Authentication to bastion servers requires a Rackspace employee to have an active account within the corporate AD.

Data center hosting services system customer devices are managed within two forests, separate from the Rackspace corporate AD network domain:

- Intensive AD: This multi-domain forest is used to authenticate Rackspace employees into the data center hosting services customer environments.

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

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

Customer environments are appropriately segregated from other customers through use of organizational units (OUs) within the Intensive and Global RS ADs.

Rackspace has established a minimum password baseline configuration for its Intensive and Global RS AD systems. Rackspace employees gain access to the customer environments using customer network passwords that are configured to expire after 10 hours. Users with administrative privileges to customer devices are provisioned credentials within the Intensive AD and specific AD groups. New user accounts within the Intensive AD are created based on a person's job function and / or manager approval.

Data center hosting services customers purchase hardware from Rackspace and are given read only access to allow full transparency into their own environment. Data center hosting services customers who have elected to use their own hardware are given full administrative control to this infrastructure. Customer firewalls and other network devices delineate the boundary between Rackspace, customer environments, and shared infrastructure. Rackspace manages customer environments following strict security guidelines and policies so as to not risk compromise of system and prevent overlap within the shared infrastructure. Rackspace fully manages the administration of shared infrastructure and Rackspace customers retain full administrative rights and control of their environments. The customer is considered the primary system administrator of their environment. The customer is considered the primary system owner of their environment as changes are not made without their documented approval within a ticket. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment. A firewall rule set can be modified by authorized Rackspace employees with terminal access controller access control system (TACACS) clearance which is checked by Cisco ACS software. These commands are authorized and accounted for via ACS.

Customer environments are isolated from one another via the use of virtual networks (VLAN) to logically separate customer traffic. VLANs are used to logically segment customers on the Rackspace network into different broadcast domains to ensure packets are switched only between ports that are designated on the same VLAN, ensuring segmentation of networks amongst Rackspace customers.

Physical Security

Rackspace uses vendors for the physical security controls at leased data centers. 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 related to Rackspace's service commitments and system requirements and, as a result, the vendors are not deemed subservice organizations and complementary subservice organization controls that are not assumed in the design of Rackspace's controls.

Rackspace implements various physical security mechanisms to protect its personnel, hardware, network, and data from damage or loss due to unauthorized access.

Documented policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews these policies and procedures on an annual basis. Physical access to the data center facilities is documented and granted based on manager approval. The Rackspace data center manager will revoke access when physical access is no longer needed due to termination of employment or services.

Management performs a review of physical access to data center facilities on at least a semi-annual basis to help ensure that access is restricted to authorized personnel.

Access to Rackspace owned data centers is restricted through the use of biometric authentication devices (e.g., hand geometry and /or iris scanner) and keycard / badge devices. Personnel are required to display their identity badges when onsite at Rackspace facilities and visitors to the data center are required to be escorted at all times. Additional physical safeguards are in place to restrict access to Rackspace owned data centers including security guards, alarm systems, and closed-circuit television (CCTV) monitoring.

Encryption and Data Destruction

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. To reinforce the objective to secure data, the secure file transfer standard and the physical media handling standard define mandatory security measures for when full encryption of removable media is required. Rackspace encrypts connections to customer portals using secure sockets layer (SSL) or TLS.

Confidential data is sanitized and removed prior to disposal of removable media that is flagged for reuse or disposal at the LON3, NYC2, and MCI1 data centers.

Change Management

A structured change management process is documented within the Rackspace Technical Change Management policy and this policy is reviewed and approved annually by the chief operating officer (COO). The purpose of this policy is to mitigate potential risk and customer impact associated with technical changes to the Rackspace production technical infrastructure.

A change is any change made to the production technical infrastructure which has the potential to impact more than one internal or external customer. This includes, but is not limited to, changes to hardware, networking, and applications. Rackspace employees who make global changes to the production technical infrastructure are expected to abide by this policy.

The change management process requires that changes that impact or have the potential to impact more than one customer are recorded and reviewed in an IT Service Management (ITSM) tool. Changes are planned, tested when technically feasible, evaluated for risk, prioritized, approved, and implemented in a controlled and consistent manner.

Prior to submitting a change, a change requester is required to review the change using the risk level assessment to determine if the risk level is low, medium, or high. The risk level determines the level of approval, the corresponding communications, and other actions required by the Racker proposing the change. The assessment consists of a risk analysis of five different dimensions: potential impact, planned impact, resiliency, past history, and likelihood.

Technical infrastructure changes with a medium risk rank can be escalated to the change sponsor for implementation approval, and technical infrastructure changes with a high risk are escalated to the change sponsor and to the change management board for implementation approval. After the change management board has reviewed changes and approved where necessary, the change is implemented. Once maintenance has been completed, if unexpected issues or failures arising during the implementation process are analyzed and reported to the change management board.

Rackspace has contractual Service Level Agreements (SLAs) in place that requires external customers receive at least a 72-hour notification for scheduled non-emergency maintenances and up to a 72-hour notice for emergency maintenances. Customers are notified via customer portal and / or other communication channels and are provided information on the effects of the changes to their operations so that they can take appropriate action.

Data Backup and Disaster Recovery

Processing capacity is monitored by data center personnel via the data center operations metrics dashboard. Additionally, data center capacity utilization is reviewed on a monthly basis by data center leadership.

Capacity management (power consumption) for customers is a view of customer environments that 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 capacity in their environment. Rackspace utilizes redundant routing and switching equipment for its core network infrastructure to protect against availability issues.

Rackspace has developed and maintains a process to address its business continuity plan (BCP) 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 BCP exists and provides the global BCP for Rackspace data centers to manage significant disruptions to its operations and infrastructure.

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

Natural disasters have the potential to disrupt data centers and systems and data housed within these systems. Backups are scheduled and performed for customers who have subscribed to the backup service. Backup utility software is used to schedule and perform backups of data on customer servers. Rackspace works with customers to establish a customized backup schedule that is specific to each customer's implementation and operations. In addition, the backup utility software performs backups according to the predefined schedule determined by the customer. Failures are monitored and e-mail alerts are generated to send to backup administrators.

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

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace utilizes an automated disc failure alert process in order to mitigate the risk of faulty media.

Environmental Security

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

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

Incident Response

Rackspace has a global security operations center (GSOC) team responsible for the identification, tracking, documentation, resolution, and communication of incidents. The incident management team facilitates the remediation and communication efforts for any incident affecting the company's products or infrastructure. Resources are engaged to help restore disrupted services and mitigate the possible adverse effects incidents can have on business operations. Leaders are provided with incident status information to make decisions and direct resources to maintain operations.

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

The GSOC has implemented several layers of security protection and defense mechanisms within the Rackspace network. The GSOC department is composed of three teams for proactive and reactive purposes: defensive infrastructure, threat and vulnerability analysis (TVA), and IR. The defensive infrastructure team deploys GSOC security sensors and collectors throughout the network. This team monitors, maintains, and provides maintenance for all security equipment globally and ensure the GSOC is equipped to handle the latest threats based on emerging and existing technology. The TVA is responsible for evaluating the infrastructure and operating systems that

support internal applications for the services offered to customers. Additionally, the TVA team provides threat intelligence for the GSOC, and Rackspace based on key relationships and vulnerability assessments performed throughout the year. Finally, the IR team monitors, detects, and responds to cyber security events. The IR team will search for malicious activity based on threat intelligence, investigate major events, and is responsible for educating Rackspace employees on safe and secure business practices.

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

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

System Monitoring

In addition, there are several mechanisms and controls in place to safeguard network security and availability. For example, the GSOC team has implemented an IDS to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks. 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. Also, Rackspace has implemented an endpoint protection solution to monitor potential threats.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer Information	Rackspace records and keeps track of customer activity in relation to the types of services customers and their users use, the configuration of their environments, and performance metrics related to service requests and the use of the services.	Confidential
User / Account Data	User accounts created for customers for use in their respective data center hosting services environments is stored in Rackspace managed systems. This data includes usernames, full customer names, and organizational information. This information is required to provision and provide services and does not include any personally identifiable information (PII), protected health information (PHI), or other sensitive data. This collection is permitted under the master service agreement (MSA) and associated product terms.	

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Log Information	Rackspace collects log data from management systems and customer environment systems. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.	Confidential
Metadata	Rackspace stores metadata consisting primarily of tags associated with customer environment information. Metadata enable customer data such as infrastructure metrics, application performance management (APM) and logs to be filtered and grouped. Metadata should not contain personal data as part of the intended use of the service.	

Subservice Organizations

The data center hosting services provided by Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution were not included within the scope of this examination.

The aforementioned data center hosting providers are responsible for providing physical safeguarding of IT infrastructure, to help ensure unauthorized access to the IT infrastructure does not occur. In addition, these data center hosting service providers are responsible for providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution, alone or in combination with controls at Rackspace, and the types of controls expected to be implemented at Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution to meet those criteria.

Control Activity Expected to be Implemented by Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution	Applicable Trust Services Criteria
Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution are expected to implement controls to ensure that the approval, removal, and periodic review of access for their personnel and the physical security over the leased data center facilities is maintained including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.	CC6.4 CC6.5
Digital Realty Trust, Equinix, Iron Mountain, and Shanghai Data Solution are expected to implement environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the data center hosting services system.