RACKSPACE US, INC.

SOC 2 REPORT

FOR

MANAGED PUBLIC CLOUD

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY

OCTOBER 1, 2022, TO SEPTEMBER 30, 2023

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of Rackspace US, Inc., user entities of Rackspace US, Inc.’s services, and other parties who have sufficient knowledge and understanding of Rackspace US, Inc.’s services covered by this report (each referred to herein as a “specified user”).

If the report recipient is not a specified user (herein referred to as a "non-specified user"), 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 Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

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

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Rackspace US, Inc.:

Scope

We have examined Rackspace US, Inc.'s ("Rackspace" or the "service organization") accompanying description of its Managed Public Cloud system, in Section 3, throughout the period October 1, 2022, to September 30, 2023 (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("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 and cloud hosting services. The description 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 presents Rackspace's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Rackspace's controls. The description 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.

The information included in Section 5, "Other Information Provided by Rackspace" is presented by Rackspace management to provide additional information and is not a part of the description. Information about Rackspace's management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

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 provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Rackspace is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

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

Inherent Limitations

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

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

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

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled “Testing Matrices.”

Opinion

In our opinion, in all material respects:

a. the description presents Rackspace’s Managed Public Cloud system that was designed and implemented throughout the period October 1, 2022, to September 30, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Rackspace’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Rackspace’s controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Rackspace’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Rackspace’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Rackspace; user entities of Rackspace's Managed Public Cloud system during some or all of the period of October 1, 2022, to September 30, 2023, business partners of Rackspace subject to risks arising from interactions with the Managed Public Cloud system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Schellman & Company, LLC

Columbus, Ohio
November 7, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Rackspace's Managed Public Cloud system, in Section 3, throughout the period October 1, 2022, to September 30, 2023 (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Managed Public Cloud system that may be useful when assessing the risks arising from interactions with Rackspace's system, particularly information about system controls that Rackspace has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("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 and cloud hosting services. The description 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 presents Rackspace's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Rackspace's controls. The description does not disclose the actual controls at the subservice organizations.

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

a. the description presents Rackspace's Managed Public Cloud system that was designed and implemented throughout the period October 1, 2022, to September 30, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Rackspace's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Rackspace's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Rackspace's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

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, 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.

Managed Public Cloud (MPC) services are provided to customers for the purposes of helping them migrate existing applications to cloud platforms (AWS, Microsoft Azure, and Google Cloud Platform (GCP), design and architect customer public cloud environments, provide tools and features to enhance the security of the cloud environments, and maintain on-going operations.

The following are offered through the MPC suite of services:

- Fanatical Support for AWS (FAWS)
- Fanatical Support for Azure (FAzure)
- Managed Services for GCP

Through these services Rackspace provides Fanatical Support for customers with applications on AWS, Microsoft Azure, and GCP. In providing these services Rackspace has developed a suite of tools that can be utilized by Rackspace personnel or by customers of the MPC services, depending upon the level of service and support requested. These tools are either hosted within Rackspace's data center hosting environment or within one of the cloud service providers.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

Security 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	· 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 event detection, investigation, and response	· 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 · Incident Response (IR) Plan and processes · Encryption standards · Change management procedures

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.

Components of the System Used to Provide the Service

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 includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the MPC 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 MPC services system. Additionally, this report does not extend to the workloads (data, files, information) sent by the MPC services system. The integrity and conformity with regulatory requirements of such data are solely the responsibilities of the applicable MPC services customer.

Infrastructure and Software

Rackspace manages and maintains infrastructure components supporting the MPC 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
- Physical and environmental security equipment at owned and operated data centers (cameras, badge readers, fire suppression)

Rackspace is responsible for the MPC 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 MPC 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 MPC 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 MPC 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 MPC 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 MPC 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 number (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.
- 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). Customer portals include the following sites:
    - Account.rackspace.com (Apollo): the user/account management portal for all MPC customers. Capabilities include the ability for MPC account administrators to configure account level settings like multi-factor-authentication, add additional users and their permissions, ability to configure federation, etc.
    - Login.Rackspace.com (Astra): MPC users use this portal as the entry point to gain access to other Rackspace portals. The login.rackspace.com portal is used for establishing/managing sessions and uses security assertion markup language (SAML) for seamless single sign on across portals.
- Encore – customer facing ticketing system, accessed through the customer portal, which provides customers ability to submit requests to Rackspace for changes to their environment. Encore is hosted in Rackspace's dedicated hosting environment.
- Boarding Pass – provides Rackers with on-demand, time bound, audited, and named access to manage customer subscriptions. It is an internal control panel that is used by Rackspace for the Fanatical Support for Azure service offering for purposes of managing customer environments, including access and administration.
- Passport – is a server access tool that was developed to provide members of the Rackspace Azure support team with on-demand, audited, secure, and streamlined access to customer servers (Window/Linux). It is an internal tool that is used by Rackspace to access MPC Azure customer's compute instances and their supporting infrastructure.
- Janus – a customer management and billing tool used for administrating MPC and for the customer to manage their own cloud estate. Janus allows customers to see, federate into and create / delete cloud accounts as well as easily interact with other Rackspace services. Additionally, Janus allows Rackers to manage services consumed, pricing, and other things like integrations with third-party software. It also handles billing for infrastructure and services for MPC customers by sending usage to our central billing system.

[Intentionally Blank]

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	Digital Realty and Equinix data center colocations Rackspace owned data centers
Production Servers	Architecture that supports the MPC services system.	CentOS Red Hat Enterprise Linux Ubuntu Linux Windows Server O/S	
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

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 Network Infrastructure

The stability of the Rackspace network (shared infrastructure and customer infrastructure) is essential to meeting the company's delivery of uptime and reliability commitments to customers. Rackspace takes measures to ensure that employees with access to the network infrastructure have an appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself. Internal tools, resources, and equipment logically reside within the corporate network. Access to these resources is limited to connections originating from within the network. Customer specific communications equipment represents the demarcation of shared infrastructure.

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 Requests and Access Revocation to Customer Environments

Rackspace policies require users to be specifically authorized to access information and system resources. Employee access to customer environments is restricted through several layers of authentication mechanisms and systems.

Rackspace access to customer environments is restricted by requiring connection to the Rackspace corporate AD network first. Customer environments are restricted to certain AD groups and a Rackspace employee must belong to the customer specific AD group in order to access a customer's environment. New users with access to customer environments are created based on job function and require manager approval. Access requests are documented and approved prior to provisioning. User privileges to the customer environment that are assigned to terminated employees are revoked as a component of the employee termination process.

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 and provides a layer of security between Rackspace infrastructure and the customer infrastructure; bastion servers enable the delivery of Rackspace services while protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific 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.

Rackspace users with access to the customer environment are reviewed on a quarterly basis to help ensure that access to systems and data is authorized. As a result of the quarterly review, access is revoked for users identified as no longer requiring access to the customer environment. Additionally, users with administrative access to Rackspace operational support tools are reviewed on a quarterly basis. This review is performed to ensure that access to change configurations and system functionality is restricted to authorized individuals. Rackspace utilizes the SailPoint tool, which automates certain review activities including those listed above as well as the automatic removal / disabling of access for accounts marked for removal.

Network Security

Rackspace implements logical access security measures to protect against threats from sources outside its system boundaries through various network security controls. A threat prevention solution that is in place to monitor and protect endpoint devices against potential threats. Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities. Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation.

Employee workstations are required to comply with security requirements outlined in the workstation security policy. Workstations are monitored for compliance to the defined security policy.

The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule. Rackspace encryption connections to Customer Portals use SSL or TLS.

Physical Security

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 a semi-annul 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 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 data center.

Change Management

There are three categories of changes relevant to the scope of this report:

- Internal changes: includes changes to tools used to support the services and changes to underlying infrastructure that is hosted in Rackspace's dedicated environment.
- Customer changes: includes changes made to a customer's public cloud environment.
- Application changes: includes changes to applications that are used to support the MPC services.

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

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

Proposed changes to technical infrastructure are assessed to determine the level of approval and communication required before implementation. An assessment rating consists of the review of the change across five dimensions: potential impact, planned impact, resiliency, past history, and likelihood. Based on this assessment, a rating of high, medium, or low is assigned. Technical infrastructure changes with a low risk require approval from only the change sponsor for changes that do not require customer communication and are escalated to the Rackspace technical change management team for changes that require customer communication. Technical infrastructure changes with a medium risk rank are escalated to the change sponsor for implementation approval, and technical infrastructure changes with a high-risk rank are escalated to the change sponsor and to the change management board for implementation approval.

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

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

After the change management board has reviewed changes and approved where necessary, the change is implemented. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the change management board. The ability to implement infrastructure changes into production is restricted to authorized personnel.

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

As it relates to patching, Rackspace leverages the update management tools provided by the cloud service providers to provide comprehensive reporting, patching, and deployment solutions. During the implementation phase, Rackspace will review customer patching requirements and make recommendations based on established best practices for securing environments. After the initial configuration, Rackspace will provide ongoing support in the form of scheduling changes, 24x7x365 alert response for failed patching or failed deployment update runs, and reports on current patch levels within customer environments. Customers are responsible for setting a recurring patching schedule, determining the order of reboot for their environment, and ensuring services are properly patched. Customers can also request ad hoc patching through a support ticket. Rackspace will not patch middleware or customer thoroughly tested in the specific environment.

Customer changes are appropriately documented within a ticket and communicated to and approved by the customer prior to being migrated to production. The customer is responsible for requesting changes in a ticket, performing any required user acceptance ticket, performing any required user acceptance testing (UAT), and for the approval of all Rackspace developed coding changes. Rackspace will migrate changes into production once customer approval is documented within the ticket.

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.

Rackspace maintains formal incident response processes concerning both corporate network incidents and incidents affecting customer solutions. 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 and have increasing levels of authority to which to appeal.

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

System Security and System Monitoring

There are several mechanisms and controls in place to safeguard network security and availability. For example, the GSOC 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. The IDS is configured to alert the GSOC team when potential network security events are identified. 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 and protect endpoint devices against 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 MPC 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.	
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.	

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
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.	Confidential

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The data center hosting services provided by Digital Realty Trust and Equinix and the cloud hosting services provided by AWS, Azure, and GCP were not included within the scope of this examination.

The aforementioned data center and cloud 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 and cloud 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, AWS, Azure, and GCP alone or in combination with controls at Rackspace, and the types of controls expected to be implemented at Digital Realty Trust, Equinix, AWS, Azure, and GCP to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Digital Realty Trust, Equinix, AWS, Azure, and GCP	Applicable Trust Services Criteria
AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6
Digital Realty, Equinix, AWS, Azure, and GCP are expected to implement controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4, CC6.5
AWS, Azure, and GCP are expected to implement controls for implementing controls for the transmission, movement, and removal of the underlying storage devices for the cloud hosting services where Rackspace systems reside.	CC6.7
AWS, Azure, and GCP are expected to implement controls for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Rackspace systems reside.	CC7.1
Digital Realty, Equinix, AWS, Azure, and GCP are expected to implement controls for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC7.2
AWS, Azure, and GCP are expected to implement controls for monitoring the logical access control systems for the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.	

CONTROL ENVIRONMENT

The control environment at Rackspace is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Rackspace's ethical and behavioral standards, how they are communicated and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of Rackspace values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Rackspace has implemented in this area are described below:

- The employee handbook addresses the following topic areas that include, but are not limited to, the following:
    - Acceptable use procedures
    - Code of business conduct and ethics
    - Internet access guidelines
    - Employment practices
- Employees are required to acknowledge their receipt and understanding of the employee handbook as a component of the new hire process.
- New employees are required to undergo a background check prior to their start date as a component of the new hire process.
- Performance reviews are conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.
- Employees are required to complete the code of business conduct and ethics training upon hire and on an annual basis thereafter.
- An employee sanction policy is in place and documented within the employee handbook detailing the implications of nonconformance.

Board of Directors and Audit Committee Oversight

The board of directors consists of members independent from management and has established sub-committees to provide oversight and monitoring of key risk areas (e.g., audit committee, compensation committee, and compliance committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives. Specific control activities that Rackspace has implemented in this area are described below:

- A board of directors is in place and exercises oversight of the development and performance of internal control.
- The board of directors has members who are independent from management and are objective in evaluations and decision making.
- Internal control metrics and external control assessment reports are communicated to the board of directors on an annual basis to help ensure that internal control responsibilities are aligned with business objectives.

Organizational Structure and Assignment of Authority and Responsibility

Rackspace's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Rackspace has developed an organizational structure suited to its needs. Rackspace's organizational structure depends, in part, on its size and the nature of its activities. Rackspace is segmented into business units. They include Dedicated Hosting (Managed Hosting), Managed Colocation, Openstack Public Cloud, Rackspace Private Cloud, Fanatical Experience® for technologies, MPC, Rackspace Application Support, Rackspace Managed Security, E-mail, and Apps. Each segment is led by a segment leader.

Rackspace considers factors including how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. Policies relating to business practices, knowledge and experience of key personnel, and resources have been established for carrying out duties. Policies and communications are in place to help ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that Rackspace has implemented in this area are described below:

- An organization chart is documented and defines the organizational structure, reporting lines, and authorities.
- Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
- Job descriptions are documented for employees and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Rackspace's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Rackspace has implemented in this area are described below:

- Employees are required to complete the code of business conduct and ethics training upon hire and on an annual basis thereafter.
- A security awareness policy is in place that identifies security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.
- Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.
- Performance reviews are conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.

Accountability

Rackspace's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management personnel's approach to taking and monitoring business risks; and management's attitudes toward information processing, accounting functions, and personnel. The management team provides overall direction, policies, and goals for the organization. In addition, management personnel review and approves process and procedure documentation. Management has an active philosophy and 'hands-on' operating style that emphasizes the responsibility and ownership of work projects and areas by individuals. Specific control activities that Rackspace has implemented in this area are described below:

- Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.
- An organization chart is documented and defines the organizational structure, reporting lines, and authorities.

- Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
- Job descriptions are documented for employees and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.
- An employee sanction policy is in place and documented within the employee handbook detailing the implications of nonconformance.

RISK ASSESSMENT

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security category.

Objective Setting

Information security risk assessments are completed by the GES governance risk and compliance team and require sign-off from leadership around the company. Leadership then makes decisions based on the evolving risk at the company. These decisions are communicated through the implementation of global strategies and process changes.

Risk Identification and Analysis

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 GES initiatives and projects. The enterprise security working group (ESWG) 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.

The risk management team evaluates the need for changes on a constant basis. This continuous evaluation serves to ensure Rackspace's commitment to security of products and services. Rackspace has defined a risk assessment approach. A security risk management plan exists and provides a methodology that defines Rackspace's risk assessment approach, how to identify risks, analyze and evaluate risk, and how to evaluate options for treatment of risks. Management identifies and rates risks.

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.

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

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. The Sarbanes-Oxley (SOX) compliance team performs a financial and fraud risk assessment during the annual planning / scoping process. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.

Risk Mitigation

Rackspace has documented policies and procedures in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as a part of the risk assessment process. Identified risks are rated using a risk evaluation process and ratings per the security risk management plan. The governance, risk, and compliance group identifies and evaluates enterprise risks on a continuous basis. Remediation plans are documented and tracked for risks that are rated higher than medium. Additionally, a disaster recovery and business continuity plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

For third parties, Rackspace has policies and procedures in place to help guide personnel in monitoring activities of third parties for compliance with objectives. Other policies and procedures in place include screening and on-boarding activities for contractors. 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. The policy and standards are reviewed and approved annually. Rackspace in-house legal counsel reviews contracts and amendments with vendors and customers. On an annual basis, security stakeholders perform a risk assessment that includes an evaluation of risks associated with vendors and business partners. Risks identified are formally documented, along with mitigation strategies, and reviewed by management. Other risk mitigation procedures include internal audit personnel reviewing external assessments of third-party vendors on an annual basis to help ensure third-party vendors maintain compliance with security commitments.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security category.

Selection and Development of Control Activities

Selecting control activities includes consideration of the relevant business processes and identified risks that require control activities. Additionally, both automated and manual controls are considered during the selection of control activities. Management also considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities. As part of this process, management also assigns risk owners to certain risks. The assigned risk owners select and develop control activities, including activities over technology, to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.

Control activities are deployed through the use of policies to establish what is expected and procedures that put policies into action. Management has documented policies and procedures that guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the intranet. Additionally, a data classification policy is formally documented that identifies the information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. Employees are held accountable for complying with these policies. An employee sanction procedure is in place that outlines the consequences for noncompliance.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Rackspace’s description of the system.

The description of the service auditor’s tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization’s description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security categories are applicable to the MPC system.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

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

Internal Communications

To ensure 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 MPC Wiki. The MPC 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. Security commitments are available to internal users on the company intranet and external customers. The GES team releases periodic communications focusing on immediate security and availability issues and enhancements in security and availability products. 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. The information security policies and procedures are in place and identify information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements. The Rackspace CSO holds a "Town Hall" meeting at least quarterly with the GES team to discuss and communicate the department's goals and expectations. The intent is to ensure alignment, understanding, and communication on the company's objectives globally. The meeting also serves as an opportunity for employees to express concerns and suggestions, or to ask questions relevant to the company's objectives. Security events, vulnerabilities, and any changes that could significantly affect the system of internal controls are communicated on a monthly basis to Rackspace executive leadership and security team. Additionally, Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.

External Communications

Communication between Rackspace and external customers is essential to the delivery of Rackspace services; thus, the company's website hosts information pertaining to these services. The Rackspace service level agreement (SLA) is communicated via the company website and includes provisions for network, hardware, and infrastructure downtime, while the Rackspace acceptable use policy (AUP) is available on the company website and lists activities not allowed by customers who are within the Rackspace network. Rackspace's commitment regarding the system's security is included in the Rackspace general terms and conditions which is available on the company website. Rackspace communicates service commitments and system requirements to third parties through the MSA, managed hosting services terms and conditions, and the hosted information addendum.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two.

The design and operating effectiveness of controls are periodically evaluated against security commitments and requirements, corrections, and other necessary actions relating to identified deficiencies are taken in a timely manner. 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.

Ongoing Monitoring

For systems and tools hosted in Rackspace's dedicated hosting environment that are within the boundaries of the MPC system, Rackspace employs multiple technologies to enable information security controls and monitoring, including the following:

- CrowdStrike Falcon Intel – provides next-generation antivirus, endpoint detection and response, and cyber threat intelligence.
- 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 – the primary source of log data and classified as Rackspace's central log repository, Splunk also functions as a SIEM tool to correlate aggregated events and alert on suspected issues on an on-going basis.
- Tripwire – file integrity monitoring (FIM) solution deployed on all in-scope servers. Support roles include real-time monitoring / alerting for the file system and applications and real-time monitoring / alerting for aggregated audit log repositories and databases.

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:

- System center operations manager (SCOM) – Microsoft product to support data center operational monitoring and maintenance of systems.
- InsightVM – Rapid7 product to provide vulnerability management for infrastructure and software components.

Separate Evaluations:

Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Appropriate levels of management review their internal controls frameworks on a quarterly basis and note any control weaknesses or material changes in controls / environment.

Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities. Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation. The threat and vulnerability analysis team conducts penetration testing on a bi-annual basis. Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.

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.

Subservice Organization Monitoring

For the Digital Realty Trust and Equinix leased data center facilities (DFW3, FRA1, FRA2, IAD3, LON5, ORD1, SYD2, and SYD4) and the AWS, Azure, and GCP cloud hosting providers, 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. At least annually, Rackspace reviews third-party assurance reports for each cloud service provider.

Evaluating and Communicating Deficiencies

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

System Incident Disclosures

No system incidents occurred that were the result of controls that were not suitably designed or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Rackspace's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the MPC system provided by Rackspace. The scope of the testing was restricted to the MPC system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2022, to September 30, 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the service commitments and system requirements are presented in the "Subservice Organizations" within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The employee handbook addresses the following topic areas that include, but are not limited to, the following: · Acceptable use procedures · Code of business conduct and ethics · Internet access guidelines · Employment practices	Inspected the employee handbook to determine that the employee handbook addressed the following topic areas that included, but were not limited to, the following: · Acceptable use procedures · Code of business conduct and ethics · Internet access guidelines · Employment practices	No exceptions noted.
CC1.1.2	Employees are required to acknowledge their receipt and understanding of the employee handbook as a component of the new hire process.	Inspected the handbook acknowledgement for a sample of employees hired during the period to determine that the employee handbook was acknowledged as a component of the new hire process for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	New employees are required to undergo a background check prior to their start date as a component of the new hire process.	Inquired of a security, risk, and compliance specialist regarding background checks to determine that new employees were required to undergo a background check prior to their start date as a component of the hiring process.	No exceptions noted.
		Inspected the completed background checks for a sample of employees hired during the period to determine that for each employee sampled a background check was completed prior to their start date as a component of the new hire process.	No exceptions noted.
CC1.1.4	Performance reviews are conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.	Inquired of a security, risk, and compliance specialist regarding performance reviews to determine that performance reviews were conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.	No exceptions noted.
		Inspected the completed performance review documentation for a sample of current employees to determine that management personnel conducted a performance review for each employee sampled during the period.	No exceptions noted.
CC1.1.5	Employees are required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	Inquired of a security, risk, and compliance specialist regarding code of business conduct and ethics training to determine that employees were required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of employees hired during the period to determine that each employee sampled completed code of business conduct and ethics training upon hire.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of current employees to determine that each employee sampled completed the code of business conduct and ethics training during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.6	An employee sanction policy is in place and documented within the employee handbook detailing the implications of nonconformance.	Inspected the employee handbook to determine that an employee sanction policy was in place and documented within the employee handbook detailing the implications of nonconformance.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	A board of directors is in place and exercises oversight of the development and performance of internal control.	Inspected the corporate governance guidelines to determine that a board of directors was in place and exercised oversight of the development and performance of internal control.	No exceptions noted.
CC1.2.2	The board of directors has members who are independent from management and are objective in evaluations and decision making.	Inspected the biographies for each board of directors' member to determine that the board of directors had members who were independent from management and were objective in evaluations and decision making.	No exceptions noted.
CC1.2.3	Internal control metrics and external control assessment reports are communicated to the board of directors on an annual basis to help ensure that internal control responsibilities are aligned with business objectives.	Inquired of a security, risk, and compliance specialist regarding board reviews of internal control metrics and external control assessment reports to determine that internal control metrics and external control assessment reports were communicated to the board of directors on an annual basis to help ensure that internal control responsibilities were aligned with business objectives.	No exceptions noted.
		Inspected the most recent board of directors' meeting minutes to determine that internal and control metrics and external control assessment reports were communicated to the board of directors during the period.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	An organization chart is documented and defines the organizational structure, reporting lines, and authorities.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure, reporting lines, and authorities.	No exceptions noted.
CC1.3.2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected security policies and organization chart to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.3	Job descriptions are documented for employees and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the job descriptions for a sample of active employment positions during the period to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Employees are required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	Inquired of a security, risk, and compliance specialist regarding code of business conduct and ethics training to determine that employees were required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of employees hired during the period to determine that each employee sampled completed code of business conduct and ethics training upon hire.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of current employees to determine that each employee sampled completed the code of business conduct and ethics training during the period.	No exceptions noted.
CC1.4.2	A security awareness policy is in place that identifies security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	Inspected the security awareness policy to determine that a security awareness policy was in place that identified security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	Inquired of a HR global compliance specialist regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for sample of new hires during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for a sample of current employees to determine that each employee sampled completed security awareness training during the period to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
CC1.4.4	Performance reviews are conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.	Inquired of a security, risk, and compliance specialist regarding performance reviews to determine that performance reviews were conducted by management personnel on at least an annual basis to help ensure employee compliance with the employee handbook and competencies.	No exceptions noted.
		Inspected the completed performance review documentation for a sample of current employees to determine that management personnel conducted a performance review for each employee sampled during the period.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls on and communicated and monitored nonconformities during the period.	No exceptions noted.
CC1.5.2	An organization chart is documented and defines the organizational structure, reporting lines, and authorities.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure, reporting lines, and authorities.	No exceptions noted.
CC1.5.3	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected security policies and organization chart to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
CC1.5.4	Job descriptions are documented for employees and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the job descriptions for a sample of active employment positions during the period to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.
CC1.5.5	An employee sanction policy is in place and documented within the employee handbook detailing the implications of nonconformance.	Inspected the employee handbook to determine that an employee sanction policy was in place and documented within the employee handbook detailing the implications of nonconformance.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Documented information security policies and procedures are in place that identify information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place that identified information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	An access control system is utilized to log administrator activity including usernames, successful and unsuccessful login attempts, and timestamps to network devices.	Inspected the access control system logging configurations and an example access log generated during the period to determine that an access control system was utilized to log administrator activity including usernames, successful and unsuccessful login attempts, and timestamps to network devices.	No exceptions noted.
CC2.1.3	The access control system logs are retained for one year.	Inspected the access control system retention configurations and an example archived access log to determine that the access control system logs were retained for one year.	No exceptions noted.
CC2.1.4	A SIEM tool is configured to log and monitor failed login attempts to the network.	Inspected the SIEM tool configurations to determine that a SIEM tool was configured to log and monitor failed login attempts to the network.	No exceptions noted.
CC2.1.5	The SIEM tool is monitored 24/7 by security personnel regarding failed login attempts to the network.	Inquired of a security, risk, and compliance management specialist regarding SIEM tool monitoring to determine that the SIEM tool was monitored 24/7 by security personnel regarding failed login attempts to the network.	No exceptions noted.
		Inspected the SIEM tool failed login attempt alert generated during the period to determine that the SIEM tool was monitored 24/7 by security personnel regarding filed login attempts to the network.	No exceptions noted.
CC2.1.6	An IDS is in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	Inspected the network diagram, the IDS systems monitored, and IDS configurations to determine that an IDS was in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	No exceptions noted.
CC2.1.7	The IDS is configured to alert the GSOC team when potential network security events are identified.	Inspected the IDS alert notification configurations and an example alert generated during the period to determine that the IDS was configured to alert the GSOC team when potential network security events were identified.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.8	A threat prevention solution is in place to monitor and protect endpoint devices against potential threats.	Inspected the threat prevention configurations for a sample of endpoint devices to determine that a threat prevention solution was in place to monitor and protect endpoint devices against potential threats for each endpoint device sampled.	No exceptions noted.
CC2.1.9	Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities.	Inspected the vulnerability scanning configurations and vulnerability scan results for a sample of months during the period to determine that vulnerability scans of the Rackspace infrastructure were performed to identify potential security vulnerabilities for each month sampled.	No exceptions noted.
CC2.1.10	Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation.	Inspected the remediation plans for a sample of vulnerabilities identified during a sample of monthly vulnerability scans to determine that remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure were documented and tracked through remediation for each identified vulnerability sampled.	No exceptions noted.
CC2.1.11	A threat and vulnerability analysis team is in place to identify potential concerns that would impair system security.	Inspected the vulnerability management standard and the threat and vulnerability team organizational chart to determine that a threat and vulnerability analysis team was in place to identify potential concerns that would impair system security.	No exceptions noted.
CC2.1.12	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC2.1.13	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls and communicated and monitored nonconformities during the period.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Documented information security policies and procedures are in place that identify information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place that identified information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	No exceptions noted.
CC2.2.2	Rackspace communicates to internal and external parties the scope of systems through compliance documents including, but not limited to, the following: · PCI AOC · ISO 27001 statement of applicability · Rackspace description of controls · Rackspace Dedicated FAQ	Inspected the most recently completed compliance documents made available on the company intranet to determine that Rackspace communicated to internal parties the scope of systems through compliance document including: · PCI AOC · ISO 27001 statement of applicability · Rackspace description of controls · Rackspace Dedicated FAQ	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.3	The MPC Wiki is made available to personnel via the company intranet and includes documented policies, procedures, contact personnel, organizational structure by region, and the scope and boundaries.	Inspected the MPC Wiki on the company intranet to determine that the MPC Wiki was made available to personnel via the company intranet and included documented policies, procedures, contact personnel, organizational structure by region, and the scope and boundaries.	No exceptions noted.
CC2.2.4	The system's security commitments are communicated to internal users via the company intranet and are included in the Rackspace general terms and conditions available to external users on the company website.	Inspected the security commitments on the company intranet to determine that the system's security commitments were communicated to internal users via the company intranet.	No exceptions noted.
		Inspected the security commitments included in the Rackspace general terms and conditions on the company website to determine that the system's security commitments were included in the Rackspace general terms and conditions available to external users on the company website.	No exceptions noted.
CC2.2.5	Employees are required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	Inquired of a security, risk, and compliance specialist regarding code of business conduct and ethics training to determine that employees were required to complete code of business conduct and ethics training upon hire and on an annual basis thereafter.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of employees hired during the period to determine that each employee sampled completed code of business conduct and ethics training upon hire.	No exceptions noted.
		Inspected the code of conduct and ethics training documentation and evidence of training completion for a sample of current employees to determine that each employee sampled completed the code of business conduct and ethics training during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.6	A security awareness policy is in place that identifies security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	Inspected the security awareness policy to determine that a security awareness policy was in place that identified security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	No exceptions noted.
CC2.2.7	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	Inquired of a HR global compliance specialist regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for sample of new hires during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for a sample of current employees to determine that each employee sampled completed security awareness training during the period to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
CC2.2.8	Documented incident response procedures are made available to personnel via the company intranet that outline the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures, and documentation requirements.	Inspected the incident response procedures to determine that documented incident response procedures were made available to personnel via the company intranet that outlined the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures and documentation requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.9	A whistleblower hotline is in place and made available to internal and external users to report security, availability, and confidentiality failures, incidents, concerns, and other complaints.	Inspected the whistleblower hotline information on the company intranet and company website to determine that a whistleblower hotline was in place and was made available to internal and external users to report security, availability, and confidentiality failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.10	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC2.2.11	The Rackspace CSO holds a town hall meeting on at least a quarterly basis with the GES team.	Inspected the town hall meeting invites and meeting minutes for a sample of quarters during the period to determine that the Rackspace CSO held a town hall meeting with the GES team for each quarter sampled.	No exceptions noted.
CC2.2.12	The GES team releases e-mail communications to employees regarding immediate security and availability issues and enhancements in security and availability products.	Inspected e-mails from the GES to employees for a sample of e-mail communications generated during the period to determine that the GES team released e-mail communications to employees regarding immediate security and availability issues and enhancements in security and availability products for each communication sampled.	No exceptions noted.
CC2.2.13	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls and communicated and monitored nonconformities during the period.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Service commitments and system requirements are communicated to third parties through the MSA, Managed Hosting Services Terms and Conditions, and / or the Hosted Information Addendum documents.	Inspected the MSA, Managed Hosting Services Terms and Conditions, and the Hosted Information Addendum templates to determine that the service commitments and system requirements were communicated to third parties through the MSA, Managed Hosting Services Terms and Conditions, and / or the Hosted Information Addendum documents.	No exceptions noted.
CC2.3.2	The system's security commitments are communicated to internal users via the company intranet and are included in the Rackspace general terms and conditions available to external users on the company website.	Inspected the security commitments on the company intranet to determine that the system's security commitments were communicated to internal users via the company intranet.	No exceptions noted.
		Inspected the security commitments included in the Rackspace general terms and conditions on the company website to determine that the system's security commitments were included in the Rackspace general terms and conditions available to external users on the company website.	No exceptions noted.
CC2.3.3	An acceptable use policy is available on the company website that lists activities not allowed by customers who are within the Rackspace network.	Inspected the acceptable use policy on the company website to determine that an acceptable use policy was available on the company website that listed activities not allowed by customers who were within the Rackspace network.	No exceptions noted.
CC2.3.4	Customer changes require approval prior to implementation.	Inquired of infrastructure change manager regarding customer changes to determine that customer changes required approval prior to implementation.	No exceptions noted.
		Inspected the change request tickets for a sample of customer changes implemented during the period to determine that customer changes required approval for each change sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.5	Documented incident response procedures are made available to personnel via the company intranet that outline the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures, and documentation requirements.	Inspected the incident response procedures to determine that documented incident response procedures were made available to personnel via the company intranet that outlined the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures and documentation requirements.	No exceptions noted.
CC2.3.6	A whistleblower hotline is in place and made available to internal and external users to report security, availability, and confidentiality failures, incidents, concerns, and other complaints.	Inspected the whistleblower hotline information on the company intranet and company website to determine that a whistleblower hotline was in place and was made available to internal and external users to report security, availability, and confidentiality failures, incidents, concerns, and other complaints.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Internal control metrics and external control assessment reports are communicated to the board of directors on an annual basis to help ensure that internal control responsibilities are aligned with business objectives.	Inquired of a security, risk, and compliance specialist regarding board reviews of internal control metrics and external control assessment reports to determine that internal control metrics and external control assessment reports were communicated to the board of directors on an annual basis to help ensure that internal control responsibilities were aligned with business objectives.	No exceptions noted.
		Inspected the most recent board of directors' meeting minutes to determine that internal and control metrics and external control assessment reports were communicated to the board of directors during the period.	No exceptions noted.
CC3.1.2	Documented policies and procedures are in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	Inquired of a security, risk, and compliance specialist regarding the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	No exceptions noted.
CC3.1.3	Security stakeholders perform a risk assessment on a continuous basis that includes an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impact security. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that included an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impacted security and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	Inquired of a security, risk, and compliance specialist regarding the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	No exceptions noted.
		Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	Security stakeholders perform a risk assessment on a continuous basis that includes an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impact security. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that included an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impacted security and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.3	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC3.2.4	The entity's information security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of a security, risk, and compliance specialist regarding monitoring of the security impact of emerging technologies and the impact of changes to applicable laws or regulations to determine that the that the entity's information security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected an example security newsletter received by the information security group during the period to determine that the entity's information security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in assessing and managing risks associated with fraud as a part of the risk assessment process.	Inquired of a security, risk, and compliance specialist regarding the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in assessing and managing risks associated with fraud as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in assessing and managing risks associated with fraud as a part of the risk assessment process.	No exceptions noted.
CC3.3.2	Security stakeholders perform a risk assessment on an annual basis that includes an evaluation of risks associated with fraud. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the most recently completed risk assessment to determine that security stakeholders performed a risk assessment during the period that included an evaluation of risks associated with fraud and risks identified were formally documented, along with mitigation strategies, and reviewed by management.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The entity's information security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of a security, risk, and compliance specialist regarding monitoring of the security impact of emerging technologies and the impact of changes to applicable laws or regulations to determine that the that the entity's information security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected an example security newsletter received by the information security group during the period to determine that the entity's information security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.4.2	A documented security risk management policy is in place to guide personnel in the risk assessment process including identifying and assessing changes that could significantly impact the system of internal control.	Inspected the security risk management policy to determine that a documented security risk management policy was in place to guide personnel in the risk assessment process including identifying and assessing changes that could significantly impact the system of internal control.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.3	Security stakeholders perform a risk assessment on a continuous basis that includes an evaluation of risks associated with changes that could significantly impact the system of internal control. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that included an evaluation of risks associated with changes that could significantly impact the system of internal control and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Documented information security policies and procedures are in place that identify information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place that identified information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	No exceptions noted.
CC4.1.2	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls and communicated and monitored nonconformities during the period.	No exceptions noted.
CC4.1.3	Management reviews third-party assurance reports on an annual basis for each cloud service provider.	Inquired of a security, risk, and compliance specialist regarding third-party assurance report reviews to determine that management reviewed third-party assurance reports on an annual basis for each cloud service provider.	No exceptions noted.
		Inspected the review of third-party assurance reports for each cloud service provider to determine that management reviewed third-party assurance reports for each cloud service provider during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	Internal control metrics and external control assessment reports are communicated to the board of directors on an annual basis to help ensure that internal control responsibilities are aligned with business objectives.	Inquired of a security, risk, and compliance specialist regarding board reviews of internal control metrics and external control assessment reports to determine that internal control metrics and external control assessment reports were communicated to the board of directors on an annual basis to help ensure that internal control responsibilities were aligned with business objectives.	No exceptions noted.
		Inspected the most recent board of directors' meeting minutes to determine that internal and control metrics and external control assessment reports were communicated to the board of directors during the period.	No exceptions noted.
CC4.1.5	The SOX team performs an assessment of the appropriateness of the control environment on a quarterly basis. Any control deficiencies identified are escalated to management and monitored through remediation.	Inquired of a security, risk, and compliance specialist regarding the SOX quarterly control assessments to determine that the SOX team performed an assessment of the appropriateness of the control environment on a quarterly basis and any control deficiencies identified were escalated to management and monitored through remediation.	No exceptions noted.
		Inspected the assessment results for a sample of quarters during the period to determine that the SOX team performed an assessment of the appropriateness of the control environment for each quarter sampled.	No exceptions noted.
		Inspected the escalation procedures and remediation for a sample of quarters during the period to determine that any control deficiencies identified were escalated to management and monitored through remediation for each quarter sampled.	No exceptions noted.
CC4.1.6	Management performs a review of the internal control framework on a quarterly basis.	Inquired of a security, risk, and compliance specialist regarding quarterly control framework reviews to determine that management performed a review of the internal control framework on a quarterly basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the internal control framework review for a sample of quarters during the period to determine that management performed a review of the internal control framework for each quarter sampled.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls and communicated and monitored nonconformities during the period.	No exceptions noted.
CC4.2.2	Internal control metrics and external control assessment reports are communicated to the board of directors on an annual basis to help ensure that internal control responsibilities are aligned with business objectives.	Inquired of a security, risk, and compliance specialist regarding board reviews of internal control metrics and external control assessment reports to determine that internal control metrics and external control assessment reports were communicated to the board of directors on an annual basis to help ensure that internal control responsibilities were aligned with business objectives.	No exceptions noted.
		Inspected the most recent board of directors' meeting minutes to determine that internal and control metrics and external control assessment reports were communicated to the board of directors during the period.	No exceptions noted.
CC4.2.3	The SOX team performs an assessment of the appropriateness of the control environment on a quarterly basis. Any control deficiencies identified are escalated to management and monitored through remediation.	Inquired of a security, risk, and compliance specialist regarding the SOX quarterly control assessments to determine that the SOX team performed an assessment of the appropriateness of the control environment on a quarterly basis and any control deficiencies identified were escalated to management and monitored through remediation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the assessment results for a sample of quarters during the period to determine that the SOX team performed an assessment of the appropriateness of the control environment for each quarter sampled.	No exceptions noted.
		Inspected the escalation procedures and remediation for a sample of quarters during the period to determine that any control deficiencies identified were escalated to management and monitored through remediation for each quarter sampled.	No exceptions noted.
CC4.2.4	Management performs a review of the internal control framework on a quarterly basis.	Inquired of a security, risk, and compliance specialist regarding quarterly control framework reviews to determine that management performed a review of the internal control framework on a quarterly basis.	No exceptions noted.
		Inspected the results of the internal control framework review for a sample of quarters during the period to determine that management performed a review of the internal control framework for each quarter sampled.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls and communicated and monitored nonconformities during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.2	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC5.1.3	Documented policies and procedures are in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in selecting and developing control activities that contributed to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process.	No exceptions noted.
CC5.1.4	Security stakeholders perform a risk assessment on a continuous basis that includes an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impact security. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that included an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impacted security and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.
		Inspected the remediation documentation for a sample of risks identified to determine that risks identified were formally documented, analyzed for significance, and reviewed by the governance, risk, and compliance group, along with mitigation strategies for each risk sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.5	The SOX team performs an assessment of the appropriateness of the control environment on a quarterly basis. Any control deficiencies identified are escalated to management and monitored through remediation.	Inquired of a security, risk, and compliance specialist regarding the SOX quarterly control assessments to determine that the SOX team performed an assessment of the appropriateness of the control environment on a quarterly basis and any control deficiencies identified were escalated to management and monitored through remediation.	No exceptions noted.
		Inspected the assessment results for a sample of quarters during the period to determine that the SOX team performed an assessment of the appropriateness of the control environment for each quarter sampled.	No exceptions noted.
		Inspected the escalation procedures and remediation for a sample of quarters during the period to determine that any control deficiencies identified were escalated to management and monitored through remediation for each quarter sampled.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Documented policies and procedures are in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives as a part of the risk assessment process.	Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives as a part of the risk assessment process.	No exceptions noted.
CC5.2.2	Security stakeholders perform a risk assessment on a continuous basis that incorporates information technology general controls. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that incorporated information technology general controls and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.3	Assigned risk owners select and develop information technology general control activities to mitigate the risks identified during the continuous risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inquired of a security, risk, and compliance specialist regarding risk mitigation strategies to determine that assigned risk owners selected and developed information technology general control activities to mitigate the risks identified during the continuous risk assessment process and the control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.
		Inspected the documented risk mitigation plans from the risk assessment for a sample of threats to determine that assigned risk owners selected and developed information technology general control activities to mitigate the risks identified during the risk assessment process and the control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold for each threat sampled.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented information security policies and procedures are in place that identify information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place that identified information required to support the functioning of internal control, achievement of objectives, and associated protection, access rights, and retention requirements.	No exceptions noted.
CC5.3.2	A security awareness policy is in place that identifies security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	Inspected the security awareness policy to determine that a security awareness policy was in place that identified security policies, standards, and procedures and required security awareness training to guide personnel in their information security responsibilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	Inquired of a HR global compliance specialist regarding security awareness training to determine that employees were required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for sample of new hires during the period to determine that each employee sampled completed security awareness training upon hire to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
		Inspected evidence of security awareness training completion for a sample of current employees to determine that each employee sampled completed security awareness training during the period to understand their obligations and responsibilities to comply with the security policies, standards, and procedures.	No exceptions noted.
CC5.3.4	An information security policy is in place and available to personnel on the company intranet and is reviewed on an annual basis.	Inspected the information security policy located on the company intranet and evidence of the policy’s review performed during the period to determine that an information security policy was in place and available to personnel on the company intranet and was reviewed during the period.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	An information security policy is in place and available to personnel on the company intranet and is reviewed on an annual basis.	Inspected the information security policy located on the company intranet and evidence of the policy’s review performed during the period to determine that an information security policy was in place and available to personnel on the company intranet and was reviewed during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Corporate Network Environment		
CC6.1.2	User access to in-scope system components is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding user access to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to in-scope system components during the period to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each employee sampled.	No exceptions noted.
CC6.1.3	User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges that were assigned to each terminated employee sampled were revoked as a component of the employee termination process for each employee sampled.	No exceptions noted.
CC6.1.4	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.	Inquired of an identity & access management engineer regarding user access reviews to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope systems was authorized.	No exceptions noted.
		Inspected the user access reviews for a sample of quarters during the period to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope system was authorized for each quarter sampled.	The test of control activity disclosed that a user access review was not performed for one of two quarters sampled.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.5	Remote access to production systems is restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	Inspected the VPN encryption and authentication configurations to determine that remote access to production systems was restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	No exceptions noted.
CC6.1.6	Authentication to the production network requires unique usernames, passwords, and MFA tokens.	Inspected the authentication standard and production network authentication configurations to determine that authentication to the production network required unique usernames, passwords, and MFA tokens.	No exceptions noted.
CC6.1.7	Authentication to the operating systems requires unique usernames and passwords.	Inspected the authentication configurations for a sample of production servers to determine that authentication to the operating systems required unique usernames and passwords for each server sampled.	No exceptions noted.
CC6.1.8	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS.	Inspected customer network device configurations for a sample of firewalls to determine that Rackspace secured access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS for each firewall sampled.	No exceptions noted.
CC6.1.9	Administrative access privileges to the in-scope network systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the identity & access management engineer to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.10	Administrative access privileges to the operating systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator listings for a sample of production servers with the assistance of a security, risk, and compliance management specialist to determine that administrative access privileges to the operating systems were restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
CC6.1.11	The ability to modify VPN configurations is restricted to authorized personnel.	Inspected the VPN administrator user access listing with the assistance of the security, risk, and compliance management specialist to determine that the ability to modify VPN configurations was restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Customer Environment		
CC6.1.12	User access to the customer environment is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding customer environment access to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to the customer environment during the period to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.
CC6.1.13	User privileges to the customer environment assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges to the customer environment assigned to each terminated employee sampled were revoked as a component of the employee termination process.	No exceptions noted.
CC6.1.14	User access privileges to the customer environment are reviewed on a quarterly basis to help ensure that access to customer environments is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that user access privileges to the customer environment were reviewed on a quarterly basis to help ensure that access to customer environments was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that user access privileges to customer environments were reviewed to help ensure that access to customer environments was authorized for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.15	Administrative access to Rackspace operational support tools is reviewed on a quarterly basis to help ensure that access to operational support tools is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that administrative access to Rackspace operational support tools was reviewed on a quarterly basis to help ensure that access to operational support tools was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that administrative access to Rackspace operational support tools was reviewed to help ensure that access to operational support tools was authorized for each quarter sampled.	No exceptions noted.
CC6.1.16	Access to customer environments is restricted via the Rackspace corporate AD network.	Inspected the corporate AD network configurations and VPN authentication configurations to determine that access to customer environments was restricted via the Rackspace corporate AD network.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
	Corporate Network Environment		
CC6.2.1	User access to in-scope system components is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding user access to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to in-scope system components during the period to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.2	User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges that were assigned to each terminated employee sampled were revoked as a component of the employee termination process for each employee sampled.	No exceptions noted.
CC6.2.3	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.	Inquired of an identity & access management engineer regarding user access reviews to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope systems was authorized.	No exceptions noted.
		Inspected the user access reviews for a sample of quarters during the period to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope system was authorized for each quarter sampled.	Refer to the test results for control activity CC6.1.4.
	Customer Environment		
CC6.2.4	User access to the customer environment is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding customer environment access to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to the customer environment during the period to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.5	User privileges to the customer environment assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges to the customer environment assigned to each terminated employee sampled were revoked as a component of the employee termination process.	No exceptions noted.
CC6.2.6	User access privileges to the customer environment are reviewed on a quarterly basis to help ensure that access to customer environments is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that user access privileges to the customer environment were reviewed on a quarterly basis to help ensure that access to customer environments was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that user access privileges to customer environments were reviewed to help ensure that access to customer environments was authorized for each quarter sampled.	No exceptions noted.
CC6.2.7	Administrative access to Rackspace operational support tools is reviewed on a quarterly basis to help ensure that access to operational support tools is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that administrative access to Rackspace operational support tools was reviewed on a quarterly basis to help ensure that access to operational support tools was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that administrative access to Rackspace operational support tools was reviewed to help ensure that access to operational support tools was authorized for each quarter sampled.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
	Corporate Network Environment		
CC6.3.1	User access to in-scope system components is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding user access to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to in-scope system components during the period to determine that user access to in-scope system components was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each employee sampled.	No exceptions noted.
CC6.3.2	User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges that were assigned to each terminated employee sampled were revoked as a component of the employee termination process for each employee sampled.	No exceptions noted.
CC6.3.3	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.	Inquired of an identity & access management engineer regarding user access reviews to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope systems was authorized.	No exceptions noted.
		Inspected the user access reviews for a sample of quarters during the period to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope system was authorized for each quarter sampled.	Refer to the test results for control activity CC6.1.4.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.4	Remote access to production systems is restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	Inspected the VPN encryption and authentication configurations to determine that remote access to production systems was restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	No exceptions noted.
CC6.3.5	Authentication to the production network requires unique usernames, passwords, and MFA tokens.	Inspected the authentication standard and production network authentication configurations to determine that authentication to the production network required unique usernames, passwords, and MFA tokens.	No exceptions noted.
CC6.3.6	Authentication to the operating systems requires unique usernames and passwords.	Inspected the authentication configurations for a sample of production servers to determine that authentication to the operating systems required unique usernames and passwords for each server sampled.	No exceptions noted.
CC6.3.7	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS.	Inspected customer network device configurations for a sample of firewalls to determine that Rackspace secured access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS for each firewall sampled.	No exceptions noted.
CC6.3.8	Administrative access privileges to the in-scope network systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the identity & access management engineer to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.9	Administrative access privileges to the operating systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator listings for a sample of production servers with the assistance of a security, risk, and compliance management specialist to determine that administrative access privileges to the operating systems were restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
CC6.3.10	The ability to modify VPN configurations is restricted to authorized personnel.	Inspected the VPN administrator user access listing with the assistance of the security, risk, and compliance management specialist to determine that the ability to modify VPN configurations was restricted to authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Customer Environment		
CC6.3.11	User access to the customer environment is granted based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.	Inquired of an identity & access management engineer regarding customer environment access to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
		Inspected access request forms for a sample of user accounts granted access to the customer environment during the period to determine that user access to the customer environment was granted based on job role and function and required a documented access request form and manager approval prior to access being provisioned for each user sampled.	No exceptions noted.
CC6.3.12	User privileges to the customer environment assigned to terminated employees are revoked as a component of the employee termination process.	Inspected the active directory access logs and systems access listings for a sample of employees terminated during the period to determine that user privileges to the customer environment assigned to each terminated employee sampled were revoked as a component of the employee termination process.	No exceptions noted.
CC6.3.13	User access privileges to the customer environment are reviewed on a quarterly basis to help ensure that access to customer environments is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that user access privileges to the customer environment were reviewed on a quarterly basis to help ensure that access to customer environments was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that user access privileges to customer environments were reviewed to help ensure that access to customer environments was authorized for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.14	Administrative access to Rackspace operational support tools is reviewed on a quarterly basis to help ensure that access to operational support tools is authorized.	Inquired of a system engineer regarding quarterly access reviews to determine that administrative access to Rackspace operational support tools was reviewed on a quarterly basis to help ensure that access to operational support tools was authorized.	No exceptions noted.
		Inspected the quarterly user access review results for a sample of quarters during the period to determine that administrative access to Rackspace operational support tools was reviewed to help ensure that access to operational support tools was authorized for each quarter sampled.	No exceptions noted.
CC6.3.15	Access to customer environments is restricted via the Rackspace corporate AD network.	Inspected the corporate AD network configurations and VPN authentication configurations to determine that access to customer environments was restricted via the Rackspace corporate AD network.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	A documented policy is in place to guide personnel in physical security and access to the data center facilities.	Inspected the physical security policy to determine that a documented policy was in place to guide personnel in physical security and access to the data center facilities.	No exceptions noted.
CC6.4.2	Management reviews the physical security policy on an annual basis.	Inquired of a security, risk, and compliance specialist regarding review of the physical security policy to determine that management reviewed the physical security policy on an annual basis.	No exceptions noted.
		Inspected the physical security policy to determine that management reviewed the physical security policy during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.3	Physical access to data center facilities is restricted by, but not limited to, the following technologies: · Proximity cards · Biometric scanners	Inquired with the project manager regarding physical security to the data center facilities to determine that access to data center facilities was restricted by but not limited to: · Proximity cards · Biometric scanners	No exceptions noted.
		Observed the physical access mechanisms for each owned data center facility to determine that access to the data center facilities was restricted by but not limited to: · Proximity cards · Biometric scanners	No exceptions noted.
CC6.4.4	Physical access to data center facilities is restricted by one or more of the following physical safeguards: · Security guards · Alarm systems · CCTV monitoring	Inquired with the project manager regarding physical security to the data center facilities to determine that access to data center facilities was restricted by one or more of the following physical safeguards: · Security guards · Alarm systems · CCTV monitoring	No exceptions noted.
		Observed the presence of physical safeguards for each owned data center facility to determine that access to the data center facilities was restricted by one or more of the following physical safeguards: · Security guards · Alarm systems · CCTV monitoring	No exceptions noted.
CC6.4.5	Physical access requests to the data center facilities are tracked and require manager approval.	Inspected the user access requests for a sample of employees granted access to the data centers during the period to determine that physical access requests to data center facilities were tracked and required manager approval for each employee sampled.	No exceptions noted.
CC6.4.6	Systems administration personnel revoke badge access rights as a component of the termination process.	Inspected the badge access listing for a sample of employees terminated during the period to determine that systems administration personnel revoked badge access rights as a component of the termination process for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.7	Management performs a review of physical access to data center facilities on a semi-annul basis to help ensure that access is restricted to authorized personnel.	Inquired of a security, risk, and compliance specialist regarding physical access reviews to determine that management performed a review of physical access to data center facilities on a semi-annul basis to help ensure that access was restricted to authorized personnel.	No exceptions noted.
		Inspected the most recently completed physical access review documentation to determine that management performed a user access review of physical access to data center facilities during the period to help ensure that access was restricted to authorized personnel.	No exceptions noted.
	Digital Realty, Equinix, AWS, Azure, and GCP are expected to implement controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Policies and procedures are in place to guide personnel in performing sanitization procedures where production data resides.	Inspected the media handling and secure files transfer policies and procedures to determine that policies and procedures were in place to guide personnel in performing sanitization procedures where production data resides.	No exceptions noted.
CC6.5.2	For devices flagged for reuse or disposal, confidential data is sanitized and removed prior to disposal of removable media.	Inspected an example disposal ticket to determine that for devices flagged for reuse or disposal, confidential data was sanitized and removed prior to disposal of removable media.	No exceptions noted.
		Observed the device sanitization and disposal process at the data center facilities to determine that for devices flagged for reuse or disposal, confidential data was sanitized and removed prior to disposal of removable media.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		
	Digital Realty, Equinix, AWS, Azure, and GCP are expected to implement controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A threat prevention solution is in place to monitor and protect endpoint devices against potential threats.	Inspected the threat prevention configurations for a sample of endpoint devices to determine that a threat prevention solution was in place to monitor and protect endpoint devices against potential threats for each endpoint device sampled.	No exceptions noted.
CC6.6.2	Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities.	Inspected the vulnerability scanning configurations and vulnerability scan results for a sample of months during the period to determine that vulnerability scans of the Rackspace infrastructure were performed to identify potential security vulnerabilities for each month sampled.	No exceptions noted.
CC6.6.3	Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation.	Inspected the remediation plans for a sample of vulnerabilities identified during a sample of monthly vulnerability scans to determine that remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure were documented and tracked through remediation for each identified vulnerability sampled.	No exceptions noted.
CC6.6.4	Remote access to production systems is restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	Inspected the VPN encryption and authentication configurations to determine that remote access to production systems was restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	No exceptions noted.
CC6.6.5	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS.	Inspected customer network device configurations for a sample of firewalls to determine that Rackspace secured access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS for each firewall sampled.	No exceptions noted.
CC6.6.6	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall ruleset to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
CC6.6.7	Rackspace encryption connections to Customer Portals use SSL or TLS.	Inspected the configuration of the Customer Portals to determine that cryptography protocols such as SSL or TLS were in place.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	AWS, Azure, and GCP are expected to implement controls for managing logical access to the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Policies are in place that prohibit the transmission of classified data over the Internet or other public communications paths unless it is encrypted.	Inspected the cryptography policy to determine that policies were in place that prohibited the transmission of classified data over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Policies and procedures are in place to guide personnel in performing sanitization procedures where production data resides.	Inspected the media handling and secure files transfer policies and procedures to determine that policies and procedures were in place to guide personnel in performing sanitization procedures where production data resides.	No exceptions noted.
CC6.7.3	Remote access to production systems is restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	Inspected the VPN encryption and authentication configurations to determine that remote access to production systems was restricted to authorized employees with a valid MFA token over an encrypted VPN connection.	No exceptions noted.
CC6.7.4	For devices flagged for reuse or disposal, confidential data is sanitized and removed prior to disposal of removable media.	Inspected an example disposal ticket to determine that for devices flagged for reuse or disposal, confidential data was sanitized and removed prior to disposal of removable media.	No exceptions noted.
		Observed the device sanitization and disposal process at the data center facilities to determine that for devices flagged for reuse or disposal, confidential data was sanitized and removed prior to disposal of removable media.	No exceptions noted.
CC6.7.5	Rackspace encryption connections to Customer Portals use SSL or TLS.	Inspected the configuration of the Customer Portals to determine that cryptography protocols such as SSL or TLS were in place.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for implementing controls for the transmission, movement, and removal of the underlying storage devices for the cloud hosting services where Rackspace systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	A threat prevention solution is in place to monitor and protect endpoint devices against potential threats.	Inspected the threat prevention configurations for a sample of endpoint devices to determine that a threat prevention solution was in place to monitor and protect endpoint devices against potential threats for each endpoint device sampled.	No exceptions noted.
CC6.8.2	Employee workstations are required to comply with security requirements outlined in the workstation security policy.	Inspected the workstation security policy to determine that guidelines related to workstation security compliance requirements were defined.	No exceptions noted.
CC6.8.3	Workstations are monitored for compliance to the defined security policy.	Inquired of a security, risk, and compliance, specialist to determine that workstations were monitored by an endpoint protection application.	No exceptions noted.
		Inspected the listing of workstations and monitoring device listing evidence and an example workstation configuration to determine that workstations were monitored for compliance.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	An IDS is in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	Inspected the network diagram, the IDS systems monitored, and IDS configurations to determine that an IDS was in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	No exceptions noted.
CC7.1.2	The IDS is configured to alert the GSOC team when potential network security events are identified.	Inspected the IDS alert notification configurations and an example alert generated during the period to determine that the IDS was configured to alert the GSOC team when potential network security events were identified.	No exceptions noted.
CC7.1.3	Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities.	Inspected the vulnerability scanning configurations and vulnerability scan results for a sample of months during the period to determine that vulnerability scans of the Rackspace infrastructure were performed to identify potential security vulnerabilities for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation.	Inspected the remediation plans for a sample of vulnerabilities identified during a sample of monthly vulnerability scans to determine that remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure were documented and tracked through remediation for each identified vulnerability sampled.	No exceptions noted.
CC7.1.5	A threat and vulnerability analysis team is in place to identify potential concerns that would impair system security.	Inspected the vulnerability management standard and the threat and vulnerability team organizational chart to determine that a threat and vulnerability analysis team was in place to identify potential concerns that would impair system security.	No exceptions noted.
	AWS, Azure, and GCP are expected to implement controls for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Rackspace systems reside.		
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Rackspace monitors controls on an annual basis and communicates and monitors nonconformities.	Inquired of a security, risk, and compliance management specialist regarding annual internal control meetings to determine that Rackspace monitored controls on an annual basis and communicates and monitors nonconformities.	No exceptions noted.
		Inspected the annual internal audit compliance schedule and nonconformities tracking documents to determine that Rackspace monitored controls on and communicated and monitored nonconformities during the period.	No exceptions noted.
CC7.2.2	An access control system is utilized to log administrator activity including usernames, successful and unsuccessful login attempts, and timestamps to network devices.	Inspected the access control system logging configurations and an example access log generated during the period to determine that an access control system was utilized to log administrator activity including usernames, successful and unsuccessful login attempts, and timestamps to network devices.	No exceptions noted.
CC7.2.3	The access control system logs are retained for one year.	Inspected the access control system retention configurations and an example archived access log to determine that the access control system logs were retained for one year.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.4	A SIEM tool is configured to log and monitor failed login attempts to the network.	Inspected the SIEM tool configurations to determine that a SIEM tool was configured to log and monitor failed login attempts to the network.	No exceptions noted.
CC7.2.5	The SIEM tool is monitored 24/7 by security personnel regarding failed login attempts to the network.	Inquired of a security, risk, and compliance management specialist regarding SIEM tool monitoring to determine that the SIEM tool was monitored 24/7 by security personnel regarding failed login attempts to the network.	No exceptions noted.
		Inspected the SIEM tool failed login attempt alert generated during the period to determine that the SIEM tool was monitored 24/7 by security personnel regarding filed login attempts to the network.	No exceptions noted.
CC7.2.6	An IDS is in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	Inspected the network diagram, the IDS systems monitored, and IDS configurations to determine that an IDS was in place to detect and act upon the detection of potential network security events due to unauthorized software or malicious attacks.	No exceptions noted.
CC7.2.7	The IDS is configured to alert the GSOC team when potential network security events are identified.	Inspected the IDS alert notification configurations and an example alert generated during the period to determine that the IDS was configured to alert the GSOC team when potential network security events were identified.	No exceptions noted.
CC7.2.8	A threat prevention solution is in place to monitor and protect endpoint devices against potential threats.	Inspected the threat prevention configurations for a sample of endpoint devices to determine that a threat prevention solution was in place to monitor and protect endpoint devices against potential threats for each endpoint device sampled.	No exceptions noted.
CC7.2.9	Vulnerability scans of the Rackspace infrastructure are performed on a monthly basis to identify potential security vulnerabilities.	Inspected the vulnerability scanning configurations and vulnerability scan results for a sample of months during the period to determine that vulnerability scans of the Rackspace infrastructure were performed to identify potential security vulnerabilities for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.10	Remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure are documented and tracked through remediation.	Inspected the remediation plans for a sample of vulnerabilities identified during a sample of monthly vulnerability scans to determine that remediation plans for potential security vulnerabilities identified by vulnerability scans of the Rackspace infrastructure were documented and tracked through remediation for each identified vulnerability sampled.	No exceptions noted.
CC7.2.11	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC7.2.12	An automated file monitoring system is utilized to send alerts to the data center operations group in the event of a disc failure.	Inspected the automated file monitoring system alerting configurations and an example alert generated during the period to determine that an automated file monitoring system was utilized to send alerts to the data center operations group in event of a disc failure.	No exceptions noted.
	Digital Realty, Equinix, AWS, Azure, and GCP are expected to implement controls for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
	AWS, Azure, and GCP are expected to implement controls for monitoring the logical access control systems for the underlying network, virtualization management, and storage devices for the cloud hosting services where the Rackspace systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	A threat and vulnerability analysis team is in place to identify potential concerns that would impair system security.	Inspected the vulnerability management standard and the threat and vulnerability team organizational chart to determine that a threat and vulnerability analysis team was in place to identify potential concerns that would impair system security.	No exceptions noted.
CC7.3.2	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.
CC7.3.3	The GES team releases e-mail communications to employees regarding immediate security and availability issues and enhancements in security and availability products.	Inspected e-mails from the GES to employees for a sample of e-mail communications generated during the period to determine that the GES team released e-mail communications to employees regarding immediate security and availability issues and enhancements in security and availability products for each week sampled.	No exceptions noted.
CC7.3.4	Documented incident response procedures are made available to personnel via the company intranet that outline the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures, and documentation requirements.	Inspected the incident response procedures to determine that documented incident response procedures were made available to personnel via the company intranet that outlined the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures and documentation requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.5	A ticketing system is utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	Inspected the incident tickets for a sample of security incidents during the period to determine that for each incident sampled a ticketing system was utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented incident response procedures are made available to personnel via the company intranet that outline the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures, and documentation requirements.	Inspected the incident response procedures to determine that documented incident response procedures were made available to personnel via the company intranet that outlined the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures and documentation requirements.	No exceptions noted.
CC7.4.2	A ticketing system is utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	Inspected the incident tickets for a sample of security incidents during the period to determine that for each incident sampled a ticketing system was utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	No exceptions noted.
CC7.4.3	Security events, vulnerabilities, and changes that could significantly affect the system of internal controls are communicated on a monthly basis to the Rackspace executive leadership and security team.	Inquired of a security, risk, and compliance management specialist regarding internal control meetings to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated on a monthly basis to the Rackspace executive leadership and security team.	No exceptions noted.
		Inspected the Rackspace executive leadership and security team meeting invites and minutes for a sample of months during the period to determine that security events, vulnerabilities, and changes that could significantly affect the system of internal controls were communicated to the Rackspace executive leadership and security team for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response procedures are made available to personnel via the company intranet that outline the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures, and documentation requirements.	Inspected the incident response procedures to determine that documented incident response procedures were made available to personnel via the company intranet that outlined the response procedures to security incidents including identifying incidents, communicating incidents, containing / remediating incidents, determining lessons learned to evaluate the effectiveness of the procedures and documentation requirements.	No exceptions noted.
CC7.5.2	A ticketing system is utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	Inspected the incident tickets for a sample of security incidents during the period to determine that for each incident sampled a ticketing system was utilized to track reported or detected security incidents and to manage system incidents, response, escalation procedures, required communications, and resolution.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change management policies and procedures are in place to guide personnel in the change request documentation, testing, and approval of infrastructure hardware and application changes.	Inspected the change management policy to determine that change management policies and procedures were in place to guide personnel in the change request documentation, testing, and approval of infrastructure hardware and application changes.	No exceptions noted.
CC8.1.2	Management reviews the change management policy on an annual basis.	Inquired of a security, risk, and compliance specialist regarding review of the change management policy to determine that management reviewed the change management policy on an annual basis.	No exceptions noted.
		Inspected the change management policy to determine that management reviewed the change management policy during the period.	No exceptions noted.
CC8.1.3	The change management board meets on a weekly basis to discuss and communicate high risk changes that affect the system.	Inquired of a security, risk, and compliance specialist regarding change management board meetings to determine that the change management board met on a weekly basis to discuss and communicate high risk changes that affect the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the change management board calendar invite and meeting minutes for a sample of weeks during the period to determine that the change management board met to discuss and communicate high risk changes that affect the system for each week sampled.	No exceptions noted.
CC8.1.4	Infrastructure software, hardware, and application changes are documented and undergo testing where technically feasible, prior to being migrated to production.	Inspected the change request tickets for a sample of infrastructure and application changes implemented during the period to determine that each change sampled was documented and underwent testing where technically feasible, prior to being migrated to production.	No exceptions noted.
CC8.1.5	Infrastructure software, hardware, and application changes require approval prior to implementation to the production environment.	Inquired of infrastructure change manager regarding infrastructure and application changes to determine that infrastructure software, hardware, and application changes required approval prior to implementation to the production environment.	No exceptions noted.
		Inspected the change request tickets for a sample of infrastructure and application changes implemented during the period to determine that infrastructure software, hardware, and application changes required approval for each change sampled.	No exceptions noted.
CC8.1.6	Customer changes require approval prior to implementation.	Inquired of infrastructure change manager regarding customer changes to determine that customer changes required approval prior to implementation.	No exceptions noted.
		Inspected the change request tickets for a sample of customer changes implemented during the period to determine that customer changes required approval for each change sampled.	No exceptions noted.
CC8.1.7	Rackspace customers are notified of changes that impact them in accordance with the change management policy.	Inspected the change management policy and customer notifications for a sample of changes impacting customers during the period to determine that for each change sampled Rackspace customers were notified of changes that impact them in accordance with the change management policy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.8	A software development platform is utilized to restrict access to application code and provide rollback capabilities.	Inspected the software development platform user listings and example rollback capability in a commit during the period to determine that a software development platform was utilized to restrict access to source code and provide rollback capabilities.	No exceptions noted.
CC8.1.9	The ability to implement infrastructure and application changes into production is restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with the ability to implement changes with the assistance of the change manager to determine that the ability to implement infrastructure and application changes into production was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	Inquired of a security, risk, and compliance specialist regarding the risk assessment policies and procedures to determine that documented policies and procedures were in place to guide personnel in identifying and assessing risks to the achievement of its objectives as a part of the risk assessment process.	No exceptions noted.
CC9.1.2	Security stakeholders perform a risk assessment on a continuous basis that includes an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impact security. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the results of the risk assessment for a sample of threats to determine that security stakeholders performed a risk assessment that included an evaluation of control activities, business and security risks, vulnerabilities, laws, and regulations, that impacted security and risks identified were formally documented, along with mitigation strategies, and reviewed by management for each threat sampled.	No exceptions noted.
CC9.1.3	Rackspace maintains cyber, facility, and business interruption insurance policies.	Inspected the cyber, facility, and business interruption insurance policies to determine that Rackspace maintained cyber, facility, and business interruption insurance policies during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.4	A documented data center business continuity plan (BCP) is in place to guide personnel in managing significant disruptions to its operations and infrastructure.	Inspected the data center business continuity plan to determine that a documented data center BCP was in place to guide personnel in managing significant disruptions to its operations and infrastructure.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Rackspace maintains a vendor management program that is reviewed and approved annually and includes, but is not limited to, the following: · Supplier relationship management policy · Supplier information security risk management program · Supplier information security requirements standards	Inspected the vendor management program documentation to determine that Rackspace maintained a vendor management program that included, but was not limited to, the following: · Supplier relationship management policy · Supplier information security risk management program · Supplier information security requirements standards	No exceptions noted.
		Inspected the vendor management program to determine that the vendor management program was reviewed and approved during the period.	No exceptions noted.
CC9.2.2	Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with vendors.	Inquired of a security, risk, and compliance specialist regarding vendor management to determine that signed nondisclosure agreements of confidentiality and protection were required before sharing information designated as confidential with vendors.	No exceptions noted.
		Inspected an example nondisclosure agreement to determine that signed nondisclosure agreements of confidentiality and protection were required before sharing information designated as confidential with vendors.	No exceptions noted.
CC9.2.3	Vendors are evaluated in accordance with the vendor screening process and approved by management personnel during the onboarding process.	Inquired of a security, risk, and compliance specialist regarding vendor evaluations to determine that vendors were evaluated in accordance with the vendor screening process and approved by management personnel during the onboarding process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vendor evaluation form for a sample of vendors to determine that each vendor sampled was evaluated in accordance with the vendor screening process and approved by management personnel.	No exceptions noted.
CC9.2.4	Management performs an assessment on an annual basis over the physical security and environmental controls onsite for each leased data center location.	Inquired of a security, risk, and compliance specialist regarding leased data center assessments to determine that management performed an assessment on an annual basis over the physical security and environmental controls onsite for each leased data center location.	No exceptions noted.
		Inspected the most recently completed vendor assessment form for a sample of leased data center locations to determine that management performed an assessment over the physical security and environmental controls onsite for each leased data center location sampled during the period.	No exceptions noted.
CC9.2.5	Management performs a vendor information security review on an annual basis to help ensure that vendors comply with the organization's requirements.	Inquired of a security, risk, and compliance specialist regarding vendor reviews to determine that management performed a vendor information security review on an annual basis to help ensure that vendors complied with the organization's requirements.	No exceptions noted.
		Inspected the most recent information security review for a sample of vendors to determine that management performed a vendor information security review during the period to help ensure that vendors complied with the organization's requirements for each vendor sampled.	No exceptions noted.
CC9.2.6	Service commitments and system requirements are communicated to third parties through the MSA, Managed Hosting Services Terms and Conditions, and / or the Hosted Information Addendum documents.	Inspected the MSA, Managed Hosting Services Terms and Conditions, and the Hosted Information Addendum templates to determine that the service commitments and system requirements were communicated to third parties through the MSA, Managed Hosting Services Terms and Conditions, and / or the Hosted Information Addendum documents.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY RACKSPACE

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4 CC6.2.3 CC6.3.3	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.	Inspected the user access reviews for a sample of quarters during the period to determine that user access privileges to in-scope production environments were reviewed on a quarterly basis to help ensure that access to in-scope system was authorized for each quarter sampled.	The test of control activity disclosed that a user access review was not performed for one of two quarters sampled.

Management's Response:

Agreed. This finding is due to an isolated incident with a legacy system that had not been fully migrated to SailPoint. Reviews for the 4th quarter were completed, however, the system that was in use had a fatal failure. The artifacts for the Q4 TACACS / Firewall reviews were not able to be obtained due to this data failure. Please note that all other quarterly access reviews were completed for 2022 Q4.

Here are the actions Rackspace is taking in response to this finding:

1. Immediate Review and Remediation: Upon receiving the audit finding, our internal audit and compliance teams conducted an immediate review of the user access review process to determine the cause of the missed review. We have identified the specific reasons behind the oversight.
2. Quarterly User Access Review: We are revising our user access review processes to ensure that they are performed as required on a quarterly basis. This includes implementing automated reminders and enhancing the documentation and tracking of these reviews.
3. Enhanced Training and Awareness: We recognize the importance of employee awareness and understanding of the user access review process. As such, we are launching a comprehensive training program to educate our team members about the significance of user access reviews and their role in maintaining security.
4. Quarterly Reporting: Going forward, we will implement a quarterly reporting process to document the completion of user access reviews. This will help us track and ensure that reviews are conducted consistently.
5. Internal Audit: The security controls in place for terminating physical access have been put on notice that the GRC team over the next 12 months will perform an independent review to assure that all user's physical access is terminated in accordance with Rackspace polices and the SOC2 control framework.

The enterprise has been migrating to SailPoint to handle the access requests and re-certifications for access control moving forward. It is our believe that with the legacy system out of production, this was a limited incident identified in this SOC reporting period.