System and Organization Controls (SOC) 1 Report

Report on Rackspace's Description of Its Information Technology General Control System for the Cloud Servers™ and Cloud Files™ and on the Suitability of the Design and Operating Effectiveness of Controls throughout the Period October 1, 2018 to September 30, 2019

Prepared in Accordance with AT-C Section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*

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

Table of Contents

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

I. REPORT OF INDEPENDENT SERVICE AUDITORS

To the Management of Rackspace Hosting, Inc.

Scope

We have examined Rackspace Hosting, Inc.'s (“Rackspace” or the “Service Organization”) description of its information technology general control system for the Cloud Servers™ and Cloud Files™ at the data centers specified in Exhibit I attached to Section II entitled “Rackspace’s Description of Its Information Technology General Control System for the Cloud Servers™ and Cloud Files™” throughout the period October 1, 2018 to September 30, 2019 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in “Rackspace’s Assertion” (the “assertion”). The controls and control objectives included in the description are those that management of Rackspace believes are likely to be relevant to user entities’ internal control over financial reporting, and the description does not include those aspects of the information technology general control system for the Cloud Servers™ and Cloud Files™ that are not likely to be relevant to user entities’ internal control over financial reporting.

The description of the information technology general control system for the Cloud Servers™ and Cloud Files™ does not include control objectives related to business process controls, automated application controls, or related to key reports produced by the Cloud Servers™ and Cloud Files™. Therefore, our examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by the Cloud Servers™ and Cloud Files™.

The information included in Section V “Other Information Provided by Rackspace" is presented by management of Rackspace to provide additional information and is not a part of Rackspace’s description of its information technology general control system for the Cloud Servers™ and Cloud Files™ made available to user entities during the period October 1, 2018 to September 30, 2019. Information about Rackspace's management’s response to control exceptions identified has not been subjected to the procedures applied in the examination of the description of the information technology general control system for the Cloud Servers™ and Cloud Files™ and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the information technology general control system for the Cloud Servers™ and Cloud Files™**.**

Rackspace uses subservice organizations for physical security and environmental controls at data centers not directly owned by Rackspace. The description in Section III includes only the control objectives and related controls of Rackspace and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Rackspace can be achieved only if complementary subservice organization controls assumed in the design of Rackspace’s controls are suitably designed and operating effectively, along with the related controls at Rackspace. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Rackspace’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

In Section II, Rackspace has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Rackspace is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditors' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2018 to September 30, 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion in Section II.

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization or a subservice organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions by the information technology general control system for the Cloud Servers™ and Cloud Files™. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization or a subservice organization may become ineffective.

Description of tests of controls

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

Basis for Qualified Opinion

Rackspace states in its description of the information technology general control system for the Cloud Servers™ and Cloud Files™ that administrative access to cloud management servers and host machines is reviewed for appropriateness on a quarterly basis. However, as noted in the description of tests of controls and results thereof, for one (1) out of two (2) sampled quarters, administrative access to cloud management servers and host machines for one (1) of three (3) groups was not performed. Therefore, the control was not operating effectively throughout the period October 1, 2018 to September 30, 2019. As a result, controls were not operating effectively to achieve the control objective "*Controls provide reasonable assurance that administration access to Cloud Servers™ is restricted to authorized individuals only to support user entities' internal controls over financial reporting*."

Opinion

In our opinion, except for the matter in the "Basis for Qualified Opinion" section above, in all material respects, based on the criteria described in Rackspace's Assertion in Section II,

a. the description fairly presents the information technology general control system for the Cloud Servers™ and Cloud Files™ that was designed and implemented throughout the period October 1, 2018 to September 30, 2019.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2018 to September 30, 2019 and subservice organizations and user entities applied the complementary controls assumed in the design of Rackspace's controls throughout the period October 1, 2018 to September 30, 2019.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2018 to September 30, 2019 if complementary subservice organization and user entity controls assumed in the design of Rackspace's controls operated effectively throughout the period October 1, 2018 to September 30, 2019.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of Rackspace, user entities of Rackspace's information technology general control system for the Cloud Servers™ and Cloud Files™ during some or all of the period October 1, 2018 to September 30, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties. If report recipients are not user entities that have contracted for services with Rackspace for the period October 1, 2018 to September 30, 2019 or their independent auditors (herein referred to as a "non-specified user") and have obtained this report, or have access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

San Antonio, Texas
December 23, 2019

1 Fanatical Place
San Antonio, TX 78218

II. RACKSPACE'S ASSERTION

We have prepared the description of Rackspace's information technology general control system for the Cloud Servers™ and Cloud Files™ (the "system") at the data centers specified in Exhibit I entitled "Rackspace's Description of Its Information Technology General Control System for the Cloud Servers™ and Cloud Files™" throughout the period October 1, 2018 to September 30, 2019 (the "description") for user entities of the system during some or all of the period October 1, 2018 to September 30, 2019, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description of the information technology general control system for the Cloud Servers™ and Cloud Files™ does not include control objectives related to business process controls, automated application controls, or key reports produced by the Cloud Servers™ and Cloud Files™. Therefore, the examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by the Cloud Servers™ and Cloud Files™.

Rackspace uses subservice organizations for physical security and environmental controls at data centers not directly owned by Rackspace. The description includes only the control objectives and related controls of Rackspace and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls at Rackspace. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Rackspace's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. the description fairly presents the system made available to user entities of the system during some or all of the period October 1, 2018 to September 30, 2019 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

(1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this

includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the service organization’s system during the period covered by the description.

iii. does not omit or distort information relevant to the service organization’s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. except for the matter described in the following paragraph, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2018 to September 30, 2019 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Rackspace’s controls throughout the period October 1, 2018 to September 30, 2019. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

The accompanying description states that administrative access to cloud management servers and host machines is reviewed for appropriateness on a quarterly basis. However, as noted in the description of tests of controls and results thereof, for one (1) out of two (2) sampled quarters, administrative access to cloud management servers and host machines for one (1) of three (3) groups was not performed. Therefore, the control was not operating effectively throughout the period October 1, 2018 to September 30, 2019. As a result, controls were not operating effectively to achieve the control objective 8 “*Controls provide reasonable assurance that administration* *access to Cloud Servers™ is restricted to authorized individuals only to support user entities' internal control over financial reporting."*

Exhibit I – In-scope Data Centers

The scope of this report pertains to the Cloud Servers™ and Cloud Files™ at the following data centers:

- DFW2
- DFW3
- HKG1
- IAD3
- LON3
- LON5
- ORD1
- SYD2

III. RACKSPACE'S DESCRIPTION OF ITS INFORMATION TECHNOLOGY GENERAL CONTROL SYSTEM FOR THE CLOUD SERVERS™ AND CLOUD FILES™

Company Overview

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

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

This report covers the Cloud Servers™ and Cloud Files™ at the following data centers:

Data Center	Location	Ownership Type	Subservice Provider
DFW2	Dallas, Texas	Operated	Not applicable
DFW3	Dallas, Texas	Operated	Not applicable
HKG1	Hong Kong, China	Leased	PCCW Solutions
IAD3	Ashburn, Virginia	Leased	Digital Realty Trust
LON3	London, United Kingdom	Owned	Not applicable
LON5	London, United Kingdom	Leased	Digital Realty Trust
ORD1	Chicago, Illinois	Leased	Digital Realty Trust
SYD2	Sydney, Australia	Leased	Digital Realty Trust

Rackspace owned or operated data centers are those for which Rackspace does not utilize a subservice provider for any services relevant to the description below.

Business Overview

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

Cloud Servers™ and Cloud Files™ Overview

Cloud offerings come in the following forms:

- Public Cloud – Multi-tenant environment with pas-as-you-go scalability
- Private Cloud – Single tenant environment with dedicated servers or virtualization
- Hybrid Cloud – Connection to public clouds, private clouds, and/or traditional dedicated servers for individual application

- Multi-Cloud – Reliance on multiple cloud providers such as AWS, Microsoft, Openstack® or VMware for multiple applications

Sub-Service Providers

For only the leased data center facilities (HKG1, IAD3, LON5, ORD1, and SYD2), Rackspace uses subservice organizations to perform control activities relating to Control Objective 2 (Physical Security). The sub-service providers include Digital Realty Trust and PCCW Solutions. The description that follows only includes the control objectives and related controls of Rackspace and excludes the control activities of physical security at these leased data center facilities. Control activities for all other control objectives for the leased data center facilities are managed by Rackspace and are included in the tests contained in this report. Rackspace has processes in place to monitor activities performed by the sub-service providers.

Description of the Control Environment, Risk Assessment, Monitoring, and Communication Processes

This section provides information about four interrelated components of internal control at Rackspace:

Control Environment

A company's internal control environment reflects the overall attitude, awareness and actions of management and the board of directors concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. The following is a description of the control environment as it pertains to Rackspace's delivery of IT hosting services.

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

Ten global functions support these segments:

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

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

Internal Controls
Rackspace management is responsible for directing and controlling operations and for establishing, communicating and monitoring policies, standards and procedures. Rackspace achieves operational and strategic compliance to the company's overall objectives through proper preparation, planning, execution and governance.

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

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

Commitment to Competence
The competence of employees is a key element of the control environment. The Human Resources Team performs a review of key talent, by individual and role, to ensure that critical talent is retained. This serves to ensure that the organizational structure is aligned in a way that will support the achievement of the company's objectives and strategies. Rackspace employs staff with high levels of technical, risk and business knowledge in order to ensure proper handling of critical issues. Rackspace is committed to the development of its employees.

This commitment to competence is expressed in the company's personnel policies and related human resource programs. Specific indicators of the commitment to personnel development include recruiting and hiring policies, investment in training and development, and performance monitoring. Rackspace's commitment to competence begins with recruiting, which is the joint responsibility of the Employee Services Department and business unit or department managers. Hiring decisions are based on various factors, including educational background, prior relevant experience, past accomplishments, and indication of integrity and ethical behavior.

Rackspace is staffed with technicians on a 24 hours, 7 days a week basis to offer assistance with customer inquiries. Rackspace maintains formal job descriptions and reviews them annually.

Risk Assessment

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

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

Rackspace manages risks on an ongoing basis through a formal risk assessment process. The Global Enterprise Security Risk Management team identifies, assesses, prioritizes, and evaluates risk based on the Security Risk Management Plan. In addition to the formal risk assessment process, managers discuss and resolve issues as they arise within their areas. Also, managers monitor and adjust the control processes for which they are responsible on an as-needed basis.

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

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

Monitoring

Monitoring is a critical aspect in evaluating whether controls are operating as intended and whether they are updated as necessary to reflect changes in the processes. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities.

Rackspace maintains a Governance, Risk and Compliance (GRC) team that carries out the monitoring of compliance with established policies and procedures. The Corporate Compliance and Enterprise Risk Steering Committee (CCERSC) is seated by members of the Executive Leadership Team and meets monthly to direct Rackspace's compliance and risk prioritization, resources, enforcement, strategy and operations. The Committee's recommendations are designed to direct activities related to legal, compliance, security, and risk management strategy, policy and standards. In addition, the Internal Audit organization performs periodic audits and assessments of the organization, including the Information Technology organization.

Rackspace monitors compliance with leading security practices and internal security policies through the routine audits and assessment of its systems and processes. Assessments are performed following applicable industry standards and third-party audit firms are engaged in the assessment when appropriate. To complement these measures, exceptions to procedural problems are logged, reported, and tracked until resolved.

Rackspace creates a series of management reports that detail efforts to provide a robust, scalable, and secure infrastructure for client organizations. The data center personnel continuously monitor processing capacity while data center power utilization metrics are distributed to Rackspace leadership on a monthly basis.

Performance metric reports include data on actual system availability compared with established service level goals and standards. Management reviews performance metric reports and takes action when appropriate.

Communication

Rackspace management realizes that effective communication with personnel is vital in order to align Rackspace business strategies and goals with operating performance. The company maintains an organizational structure to properly delineate reporting within each department and job responsibility, and organizational values and behavioral standards are communicated to personnel via Rackspace's Intranet and the Rackspace Employee Handbook. The Employee Handbook is signed by new hires on their hiring date and a Code of Conduct Agreement is distributed to employees upon hiring.

Rackspace supports customer satisfaction by monitoring customer communication and issue resolution. Customer communication is handled through the Rackspace customer portal (MyRackspace™ portal) and through the company's website which hosts and communicates our commitment to availability as stated in the Service Level Agreement and our commitment to security included in the General Terms and Conditions. Rackspace communicates changes to customers' environment in a timely manner depending on the nature of the control giving as much notice as is possible and practical.

Rackspace personnel can access key performance metrics using the Rackspace Data Warehouse on a real time basis. Members of management from across several functional divisions participate in weekly meetings to discuss the status of service delivery or other matters of interest and concern. Issues or suggestions identified by personnel are readily brought to the attention of management to be addressed and resolved.

In addition, a Weekly Activity Report is shared across functional teams in order to keep Rackers apprised of current status on security and availability initiatives.

Rackspace provides ongoing security awareness guidance and information on securing data, assets, and other sensitive information to Rackspace personnel via security awareness emails sent throughout the year. Changes and updates to the security policy are communicated to employees through company-wide email and through the Global Enterprise Security department. Furthermore, Rackspace employees are trained on the Code of Business Conduct and Ethics annually.

New employees are briefed on the Rackspace security policy during the employee new hire process and each employee signs a security acknowledgement form and confidentiality agreement.

Control Objectives and Controls for IT

The description that follows outlines the processes and controls that are performed by Rackspace. This should be read in conjunction with the detailed control objectives and control activities described in Section IV that are intended to be incorporated herein by reference.

Organizational Security
Rackspace policies dictate the company's organizational values, behavioral standards, and security practices to protect access to data and systems. The Information Technology policy is established, periodically reviewed, and communicated to personnel across various communication channels. The Standards dictate the controls to be implemented for the Rackspace system. These controls are tested as part of a continuous improvement schedule and results are distributed to management for ownership and remediation as part of the overall risk management program.

Rackspace's pledge to security is reflected in an enterprise commitment to an ISO 27001 security framework. An Information Security Policy is in place and available to personnel on the company intranet. Reviews are conducted at least annually and updates are performed as needed **(SOC 1.01)**. Rackspace has instituted a Security Awareness Policy and the workforce is trained on security expectations annually **(SOC 1.02)**. Additionally, Corporate Security periodically releases notification e-mails to focus on immediate security issues, enhancements in security products, and concerns to all employees. Security commitments are available to internal users on the company intranet and external customers **(SOC 1.03)**.

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

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

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 **(SOC 2.01)**. Physical access to data center facilities is documented and granted based on manager approval **(SOC 2.02)**. The subservice organization or Rackspace Data Center manager will revoke access when physical access is no longer needed due to termination of employment or services. Physical access is disabled within 24 business hours of notification **(SOC 2.03)**.

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

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

Customers are responsible for implementing physical security controls and environmental controls to protect workstations, servers, and communication hardware that interface with their managed hosting environment at Rackspace and are housed in their facilities or other locations under their control or supervision.

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

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

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

Proposed non-emergency changes that are scored as high priority 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 rated medium or high is performed once the Change Sponsor has developed a test plan, relevant technical personnel have vetted this plan, and all necessary equipment is obtained.

Rackspace customers are notified of changes in accordance with the Change Management Policy **(SOC 3.03)** 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 non-service disruptive changes and customers are given at least 10 days' notice for non-emergency scheduled changes that could be disruptive to service. Rackspace also communicates to customers of scheduled downtime emergency changes, and of 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 migrated into the production environment. Once maintenance has been completed, unexpected issues or failures arising during the implementation process are analyzed and reported to the Change Management Board.

Incident Management

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

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

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

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

Logical Access to Network Infrastructure

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

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

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

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

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

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

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

New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval **(SOC 5.04)**. Human Resources is the only division authorized to request corporate network accounts for new employees. The request is initiated by adding a job position within the Global People System (GPS – HR database) to reflect the hire of a new employee. The Corporate Active Directory synchronizes with the GPS system every night to determine newly hired employees in need of a network account. Upon receiving Active Directory credentials, a new employee's manager is responsible for initiating an access request for any elevated or administrative access. Prior to December of 2018, access requests were created using the ServiceNow ticketing system.

In December of 2018, access requests were transitioned to go through the SailPoint tool. Users request access to onboarded groups through the SailPoint tool which are then reviewed and approved/rejected within the tool. Following approval through SailPoint, workflow will automatically add users to the approved group, thereby allowing access.

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

Since administrative access to the network is granted and managed by adding the employee's network account into an AD group or several groups, management has implemented a process to review each of the members of a group by the group owner to ensure access is still appropriate. Users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed on a quarterly basis. Any discrepancies found are corrected in a timely manner **(SOC 5.05)**. Following the implementation of SailPoint, an automated workflow is used to initiate the review and send automatic reminders to group owners.

The Corporate Active Directory- GPS synchronization also searches for terminated employees whose access needs to be removed from the network. This process ensures that Rackspace Corporate Active Directory access is disabled in a timely manner **(SOC 5.06)** for employees who are no longer with the company.

Segregation of Cloud Servers™ Customer Environments

Two factor authentication is required for remote employees to access the Cloud Servers internal network **(SOC 6.01)**. Customers can log in to Cloud Servers™ through the customer portal or through an Application Programming Interface (API). Cloud Server customers are authenticated via the Cloud Authentication System **(SOC 6.02)**. The basic function of the authentication service is to validate a client's credentials. If a client offers valid credentials, successful authentication returns a token that is used as evidence that the client's identity has already been authenticated. A token is an opaque string that represents an authorization to access cloud resources. A customer authentication token to access the cloud service is valid for a maximum of 24 hours. After session expiration, re-authentication is required **(SOC 6.03)**. A Rackspace authentication token is unique to a single customer **(SOC 6.04)**.

Each cloud server is built and resources are allocated during an automated build process initiated at the time of the customer's purchase based on the customer's specifications. During the purchase process, the specified components (e.g. RAM) determine the resource allocation for RAM, vCPU (Virtual Central Processing Unit), and disk space. The associated cloud server build script is configured with this detailed information that is stored in a customer specific configuration file.

Resources are explicitly allocated to each cloud server and segregated from other Cloud Servers on the same host machine **(SOC 6.05)**.

When a customer deletes its virtual machine in First Gen, there is a grace time period, before data is overwritten, to allow the customer the ability to restore the VM in case of accidental deletion. Once the grace period has concluded, the sector where the slice used to reside is overwritten with zeroes.

When a customer instance is deleted in Next Gen, the customer's VHD (virtual disk file) is removed. Openstack®® uses dynamically allocated VHDs. Dynamic disks are disks that allocate space on the fly based on usage, in contrast to mapping customer data 1:1 to the physical hard disk. Due to the dynamic allocation of disk space, when the customer's virtual disk file is deleted, it is impossible to find leftover data from a former customer's virtual machine. For accountability purposes, records of customers' successful and failed logins are kept for at least 90 days, as well as VM creation and deletion timestamp.

Rackspace customers can select the physical/geographical location of the data storage when spinning up a new instance and later in time if the customer wants to confirm where his/her data resides, the physical/geographical location of a tenant's data is accessible to the customer via the customer portal.

Segregation of Cloud Files™ Customer Environments

Two factor authentication is required for remote employees to access the Cloud Files internal network **(SOC 7.01)**. Rackspace offers Cloud Files™ technology powered by Openstack® to allow Cloud Files users to store/retrieve files via a simple Web Service (REST: Representational State Transfer) API, the Rackspace cloud control panel, or the MyRackspace® customer portal. Files can range in size from a few bytes up to extremely large files and the storage grows or shrinks based on the user's usage needs.

Customers can log in to Cloud Files through the customer portal or through an API. Cloud Files customers are authenticated via the Cloud Authentication System **(SOC 7.02)**, which functions as the authentication service to validate a customer's credentials. If a customer offers valid credentials, successful authentication returns a token which is used as evidence that the client's identity has already been authenticated. A token is an opaque string that represents an authorization to access cloud resources. Tokens may be revoked at any time and are valid for a finite duration. A customer's authentication token to access the cloud service is valid for a maximum of 24 hours. After session expiration, re-authentication is required.

Successful authentication returns a token with specified authorization to determined files authorized to read. File association with the customer account restricts access to files **(SOC 7.03)**. An authentication token is unique to a single customer **(SOC 7.04)**. For accountability purposes, customer logs include username, file creation and deletion timestamp, and successful or failed access attempts are kept for at least 90 days.

Rackspace customers can select the physical/geographical location of the data storage when spinning up a new Cloud Files™ instance and later in time if the customer wants to confirm where his/her data resides the physical/geographical location of a tenant's data is accessible to the customer via the customer portal.

Cloud Servers™ Administration

Rackspace customers retain full root access to their cloud servers. The customer is therefore considered the primary system administrator of their environment. Rackspace policies require Rackspace employees to be specifically authorized to access information and system resources, except for certain specified data available to all employees.

Administrator access to cloud management servers and host machines is limited to authorized Rackspace employees through the use of Corporate Active Directory groups. Only employees who have daily job functions that could include administration and troubleshooting of the cloud server environments have access to host machines or network devices. New users with administrative access to cloud management servers and host machines are created based on job function and manager approval **(SOC 8.01)**.

Administrative access to cloud management servers and host machines is reviewed for appropriateness on a quarterly basis **(SOC 8.02)**. Rackspace Corporate Active Directory access is disabled in a timely manner **(SOC 8.03)**, thereby removing administrative access to cloud management servers and host machines.

Cloud Files™ Administration

Rackspace customers retain full root access to their cloud files. The customer is therefore considered the primary system administrator of their environment. Rackspace policies require Rackspace employees to be specifically authorized to access information and system resources, except for certain specified data available to all employees.

New users with administrative access to cloud file management servers and host machines are created based on job function and manager approval. **(SOC 9.01)**. For Cloud Servers, access is administered via an automated LDAP process. Cloud File access is manually managed via role through configuration management of the files associated with administration through a Balabit server and individual system user accounts. Administrative access to Cloud Files requires authentication through a Balabit authentication server **(SOC 9.02)**.

Administrative access to cloud file management servers and host machines is reviewed for appropriateness on a quarterly basis **(SOC 9.03)**. Rackspace Corporate Active Directory access is disabled in a timely manner **(SOC 9.04)**, thereby removing administrative access to cloud file management servers and host machines.

Cloud Servers™ and Cloud Files™ Significant Events and Changes

Other than the migration to the SailPoint Identity Access Management tool in December of 2018 described above, there were no other significant changes that occurred to Cloud Servers™ and Cloud Files™ for the period October 1, 2018 to September 30, 2019.

Complementary Subservice Organization Controls

Rackspace's controls related to the Information Technology General Control System for Cloud Servers™ and Cloud Files™ cover only a portion of overall internal control for each user entity of Rackspace. It is not feasible for the control objectives related to the Information Technology General Control System for Cloud Servers™ and Cloud Files™ to be achieved solely by Rackspace. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with Rackspace's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls (CSOC) expected to be implemented at the subservice organizations as described in the table below.

Reference	Subservice Organization(s)	Complementary Subservice Organization Controls (CSOCs)	Related Control Objective
1	Digital Realty Trust	Responsible for maintaining physical security over the IAD3, LON5, ORD1, and SYD2 leased data center facilities.	2
2	PCCW Solutions	Responsible for maintaining physical security over the HKG1 leased data center facility.	2

Complementary User Entity Controls

In designing its system, Rackspace has contemplated that certain complementary controls will be implemented by user organizations to achieve certain control objectives included in this report.

This section highlights other internal control considerations that Rackspace recommends each client undertake. Clients must evaluate their own internal controls to determine if the following procedures are in place to ensure a reliable communications system between themselves and Rackspace. User auditors should determine whether user entities have established controls to provide reasonable assurance that control objectives are met through application of the following activities:

1. Customers are responsible for providing security awareness training to their employees and implementing Security leading practices (Control Objective 1 – Organizational Security).

2. Customers are responsible for establishing physical security protections over all workstations, servers, and communication hardware that interface with their managed hosting environment and that are housed in their facilities or other locations under their control or supervision (Control Objective 2 – Physical Security).

3. Customers are responsible for providing Rackspace a list of individuals with authorized access to data center facilities (Control Objective 2 – Physical Security).

4. Customers are responsible for implementing a process to request access to Rackspace data center facilities (Control Objective 2 – Physical Security).

5. Customers are responsible for establishing a process to monitor and review the customer portal for maintenance notifications and alerts (Control Objective 3 – Infrastructure Maintenance and Change Management, Control Objective 4 – Incident Management).

6. Upon notification, customer is responsible for appropriate and timely action based on the notifications that are sent (Control Objective 3 – Infrastructure Maintenance and Change Management, Control Objective 4 – Incident Management).

7. Customers are responsible for establishing a process to administer logical access to the MyRackspace™ portal (Control Objective #6 - Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments).

8. Customers are responsible for monitoring access and usage of customer applications hosted within the Rackspace environment (Control Objective 6 – Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments).

9. Customers are responsible for administering user accounts within the Cloud customer portal (Control Objective 6 – Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments, Control Objective 8 – Cloud Servers™ Administration, and Control Objective 9 – Cloud Files™ Administration).

10. Customers are responsible for administering local user and administrative operating system accounts (Control Objective 6 – Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments, Control Objective 8 – Cloud Servers™ Administration, and Control Objective 9 – Cloud Files™ Administration).

11. Customers are responsible for the configuration and management of the local operating system on their cloud server (Control Objective 6 – Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments, Control Objective 8 – Cloud Servers™ Administration, and Control Objective 9 – Cloud Files™ Administration).

12. Customers are responsible for obtaining, monitoring, and appropriately using SSL encryption certificates, if needed (Control Objective 6 – Segregation of Cloud Servers™ Customer Environments, Control Objective 7 – Segregation of Cloud Files™ Customer Environments, Control Objective 8 – Cloud Servers™ Administration, and Control Objective 9 – Cloud Files™ Administration).

IV. RACKSPACE'S CONTROL OBJECTIVES AND CONTROLS, AND PRICEWATERHOUSECOOPERS' TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

In this section, Rackspace has specified the control objectives that it believes are relevant to its clients and their auditors, and has identified its controls in place to achieve those objectives. For each control objective, there is a description of the controls that are designed to achieve it. Also, PricewaterhouseCoopers LLP, Rackspace's independent service auditor, has performed testing of the controls and presents its findings. Additionally, observation and inspection procedures were performed by PricewaterhouseCoopers as it relates to system-generated reports, queries, and listings within management's description to assess the completeness and accuracy (reliability) of the information utilized in the performance of PricewaterhouseCoopers' testing of the control activities.

Test Descriptions

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

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

Control Objective 1: Organizational Security

Controls provide reasonable assurance that security policies and procedures are implemented and communicated to stakeholders.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 1.01	An Information Security Policy is in place and available to personnel on the company intranet. Reviews are conducted at least annually and updates are performed as needed.	Inspected the Information Security Policy to determine whether it was in place and available to personnel on the company intranet. Inspected evidence to determine whether the Information Security Policy was reviewed within the last year.	No exceptions noted. No exceptions noted.
SOC 1.02	Rackspace has instituted a Security Awareness Policy, and the workforce is trained on security expectations annually.	Inspected evidence that a Security Awareness Policy was in place. For a sample of employees, inspected evidence to determine whether the workforce was trained at least annually on security expectations.	No exceptions noted. No exceptions noted.
SOC 1.03	Security commitments are available to internal users on the company intranet and external customers.	Inspected evidence that security commitments were in place and available to users on the company intranet. Inspected evidence that security commitments were in place and available to external customers.	No exceptions noted.

Control Objective 2: Physical Security

Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized and appropriate personnel.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 2.01	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 the policies and procedures on an annual basis.	Inspected the physical security policies and procedures to determine whether processes were in place to guide employees in the granting, controlling, and monitoring of physical access to Rackspace owned data centers.	No exceptions noted.
		Inspected evidence to determine whether the physical security policies and procedures were reviewed on an annual basis.	No exceptions noted.
SOC 2.02	Physical access to data center facilities is documented and granted based on manager approval.	For a sample of physical access granted to data center facilities, inspected evidence to determine whether physical access was documented and approved.	No exceptions noted.
SOC 2.03	Physical access is disabled within 24 business hours of notification.	For a sample of terminated employees, inspected badge history within the badge access system to determine whether access was disabled within 24 business hours of notification.	No exceptions noted.
SOC 2.04	Appropriateness of physical access to data center facilities is reviewed on an annual basis.	For each in-scope data center facility, inspected evidence to determine whether an annual review of appropriateness of physical access was performed; and if follow-up actions were requested, selected a sample to determine that they were completed.	No exceptions noted.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 2.05	Physical safeguards are in place to restrict access to Rackspace owned and operated data centers including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.	Observed an attempt to gain access to each owned and operated data center without a proximity card.	No exceptions noted.
		Observed an authorized individual access each owned and operated with a proximity card.	No exceptions noted.
		Observed the presence of physical safeguards outside the server room for each owned and operated data center to determine whether access was appropriately restricted.	No exceptions noted.

Complementary Subservice Organization Controls

Digital Realty Trust, and PCCW Global are responsible for maintaining physical security over the leased data centers facilities (HKG1, IAD3, LON5, ORD1, and SYD2) that host Cloud Servers™ and Cloud Files™.

Control Objective 3: Infrastructure Maintenance and Change Management

Controls provide reasonable assurance that changes to shared infrastructure software and hardware are appropriately documented, tested (when feasible), approved prior to being implemented into the production environment, and communicated to relevant parties to support user entities' internal control over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 3.01	A documented change management policy is in place and reviewed on an annual basis.	Inspected the Change Management Policy to determine whether it was in place and available to personnel on the company intranet.	No exceptions noted.
		Inspected evidence to determine whether the Change Management Policy was reviewed on an annual basis.	No exceptions noted.
SOC 3.02	Infrastructure software and hardware changes are documented, undergo testing when technically feasible, and are approved prior to being migrated to production.	For a sample of changes, inspected evidence to determine whether changes were documented, tested when technically feasible, and approved prior to being migrated to production.	No exceptions noted.
SOC 3.03	Rackspace customers are notified of changes in accordance with the Change Management Policy.	For a sample of customer changes, inspected evidence to determine whether customers were notified of changes in accordance with the Change Management Policy.	No exceptions noted.

Control Objective 4: Incident Management

Controls provide reasonable assurance that incidents including security and operational disruptions are identified, tracked, documented, resolved, and communicated to relevant parties to support user entities' internal control over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 4.01	Incident response processes exist to respond to and document problems and incidents including security and operational disruptions, establish point(s) of contact and a threshold of incident levels, and are available to personnel through the intranet.	Inspected the incident management processes to determine whether processes were in place, established point(s) of contact and thresholds of incident levels, and were available to personnel through the intranet.	No exceptions noted.
SOC 4.02	Once an incident occurs, a ticket is created to track the event, a communication is sent to applicable Rackspace personnel and customers (as necessary), and upon resolution the ticket is closed. Escalation procedures are determined and communicated to the customer (as necessary).	For a sample of incidents, inspected the corresponding incident ticket to determine whether a ticket was created to track the event, a communication was sent to applicable Rackspace personnel and customers (as necessary), and the ticket was closed upon resolution.	No exceptions noted.

Control Objective 5: Logical Access to Network Infrastructure

Controls provide reasonable assurance that logical access to network infrastructure is restricted to authorized and appropriate users to support user entities' internal control over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 5.01	Two factor authentication is used to remotely connect to the Rackspace Corporate Network.	Observed a Rackspace employee unsuccessfully connect to the Rackspace Corporate Network without utilizing two factor authentication.	No exceptions noted.
		Observed a Rackspace employee successfully connect to the Rackspace Corporate Network utilizing two factor authentication.	No exceptions noted.
		Inspected the configuration that requires users to authenticate through a VPN.	No exceptions noted.
SOC 5.02	Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS.	For a sample of customer firewalls, inspected the firewall configuration and determined whether inherent access control functionality in Cisco ACS was utilized.	No exceptions noted.
SOC 5.03	Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system.	Inspected the Default Domain Policy and compared it to Rackspace's Authentication Standard to determine whether Rackspace has established a minimum password baseline configuration for its Corporate Active Directory system.	No exceptions noted.
SOC 5.04	New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval.	For a sample of new administrators, inspected evidence to determine whether access was based on job function and manager approval.	No exceptions noted.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 5.05	Users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed on a quarterly basis.	For a sample of quarterly reviews of users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations, inspected evidence to determine whether the review was performed; and if follow-up actions were requested, selected a sample to determine that they were completed.	No exceptions noted.
SOC 5.06	Rackspace Corporate Active Directory access is disabled in a timely manner.	For a sample of terminated employees, inspected access logs to determine whether the users' access was disabled timely.	No exceptions noted.

Control Objective 6: Segregation of Cloud Servers™ Client Environments

Controls provide reasonable assurance that Cloud Servers™ customers are authenticated and segregated properly to support user entities' internal control over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 6.01	Two factor authentication is required for remote employees to access the Cloud Servers internal network.	Observed an attempt to remotely log into the Cloud Server internal network without connecting to VPN to determine whether the connection was unsuccessful Observed an attempt to log into the Cloud Server internal network while connected to VPN to determine whether the connection was successful.	No exceptions noted. No exceptions noted.
SOC 6.02	Cloud Server customers are authenticated via the Cloud Authentication System.	Observed the authentication process for a sampled customer account and determined the Cloud Authentication System was used.	No exceptions noted.
SOC 6.03	A customer's authentication token to access the cloud service is valid for a maximum of 24 hours. After token expiration, re-authentication is required.	Observed a sampled customer account authenticate to the cloud service to determine whether the customer's token expired within 24 hours +/- 30 minutes.	No exceptions noted.
SOC 6.04	A Rackspace authentication token is unique to one customer.	Observed a customer account authenticate to determine whether the token was unique to the customer.	No exceptions noted.
SOC 6.05	Resources are explicitly allocated to each cloud server and segregated from other Cloud Servers on the same host machine.	For a sample of cloud servers, inspected configurations to determine whether virtual machines and discs were logically segregated.	No exceptions noted.

Control Objective 7: Segregation of Cloud Files™ Client Environments

Controls provide reasonable assurance that Cloud Files™ customers are authenticated and segregated properly to support user entities' internal controls over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 7.01	Two factor authentication is required for remote employees to access the Cloud Files internal network.	Observed an attempt to remotely log into the Cloud Files internal network without connecting to VPN to determine whether the connection was unsuccessful. Observed an attempt to log into the Cloud Files internal network while connected to VPN to determine whether the connection was successful.	No exceptions noted. No exceptions noted.
SOC 7.02	Cloud Files customers are authenticated via the Cloud Authentication System.	Observed the authentication process for a sampled customer account and determined the Cloud Authentication System was used.	No exceptions noted.
SOC 7.03	File association with the customer account restricts and segregates access to customer files.	Observed a user access the Cloud Files system to determine whether access to files was restricted and segregated by customer account token.	No exceptions noted.
SOC 7.04	A Rackspace authentication token is unique to a single customer.	Observed a customer account authenticate to determine whether the token was unique to the customer.	No exceptions noted.

Control Objective 8: Cloud Servers™ Administration

Controls provide reasonable assurance that administration access to Cloud Servers™ is restricted to authorized individuals only to support user entities' internal controls over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 8.01	New users with administrative access to cloud management servers and host machines are created based on job function and manager approval.	For a sample of new users with administrative access to cloud management servers and host machines, inspected evidence to determine whether users were created based on job function and manager approval.	No exceptions noted.
SOC 8.02	Administrative access to cloud management servers and host machines is reviewed for appropriateness on a quarterly basis.	For a sample of quarterly reviews of administrative access to cloud management servers and host machines, inspected evidence to determine whether the review was performed; and if follow-up actions were requested, selected a sample to determine that they were completed.	**Exception noted.** For one (1) out of two (2) sampled quarters, administrative access to cloud management servers and host machines for one (1) of three (3) groups was not performed.
SOC 8.03	Rackspace Corporate Active Directory access is disabled in a timely manner.	For a sample of terminated employees, inspected access logs to determine whether the users' access was disabled timely.	No exceptions noted.

Control Objective 9: Cloud Files™ Administration

Controls provide reasonable assurance that administration access to Cloud Files™ is restricted to authorized individuals only to support user entities' internal controls over financial reporting.

Ref	Description of Controls	Tests of Operating Effectiveness	Results of Testing
SOC 9.01	New users with administrative access to cloud file management servers and host machines are created based on job function and manager approval.	For a sample of new users with administrative access to cloud file management servers and host machines, inspected evidence to determine whether users were created based on job function and manager approval.	No exceptions noted.
SOC 9.02	Administrative access to Cloud Files requires authentication through a Balabit authentication server.	Inspected system configuration to determine whether administrative access to Cloud Files required authentication thru a Balabit authentication server.	No exceptions noted.
SOC 9.03	Administrative access to cloud file management servers and host machines is reviewed for appropriateness on a quarterly basis.	For a sample of quarterly reviews of administrative access to cloud file management servers and host machines, inspected evidence to determine whether the review was performed; and if follow-up actions were requested, selected a sample to determine that they were completed.	No exceptions noted.
SOC 9.04	Rackspace Corporate Active Directory access is disabled in a timely manner.	For a sample of terminated employees, inspected access logs to determine whether the users' access was disabled timely.	No exceptions noted.

V. OTHER INFORMATION PROVIDED BY RACKSPACE

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

Management's Response to Exceptions

Ref	Control Exception Noted	Management's Response to Exceptions
SOC 8.02	For one (1) of two (2) sampled quarters, administrative access to cloud management servers and host machines for one (1) of three (3) groups was not performed.	Management has performed the following as it relates to this control exception: • Rackspace Management determined that the root cause of the exception was due to manual error and oversight during a transition of responsibilities over the review process. • Management subsequently performed a comprehensive review of individuals with administrative access to the cloud management servers and host machines environment and determined administrative access to be appropriate. • Additional testing performed by Rackspace Management subsequent to the exception identified has not found any additional instances where access was not reviewed quarterly.

(This page has been intentionally left blank.)