rackspace®

System and Organization Controls (SOC) 3 Report

Report on Rackspace's Data Center Hosting Services System Relevant to Security and Availability

For the period October 1, 2018 to September 30, 2019

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

Table of Contents

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") accompanying assertion titled "Management of Rackspace's Assertion" (assertion) that the controls within Rackspace's Data Center Hosting Services System (system) were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Rackspace's service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Rackspace's Data Center Hosting Services System were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PriceWaterhouse Coopers LLP

San Antonio, Texas
February 6, 2020

MANAGEMENT OF RACKSPACE'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Rackspace's Data Center Hosting Services System (system) throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that Rackspace's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Rackspace's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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

We assert that the controls within the system were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria.

ATTACHMENT A – RACKSPACE'S DESCRIPTION OF THE DATA CENTER HOSTING
SERVICES SYSTEM

A. System Overview

Company Background
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®.

Data Center Hosting Services Overview
Rackspace serves a broad range of customers with diverse hosting needs and requirements. Rackspace is segmented into business units. They include:

- Dedicated Hosting (Managed Hosting);
- Managed Colocation;
- Cloud;
- Fanatical Support® for technologies; and
- E-mail and Apps.

Managed Colocation serves clients that have significant in-house expertise and only require support around physical infrastructure. Rackspace Hybrid Hosting offers a combination of hosting services that enables customers to use managed hosting and cloud services under one account. Rackspace Fanatical Support® for technologies includes in-house expertise in support of AWS, VMware, Microsoft, OpenStack and others. Cloud Hosting serves clients' scalable IT-enabled capabilities using Internet technologies. The scope of this report only pertains to the Dedicated Hosting business unit and not the other services.
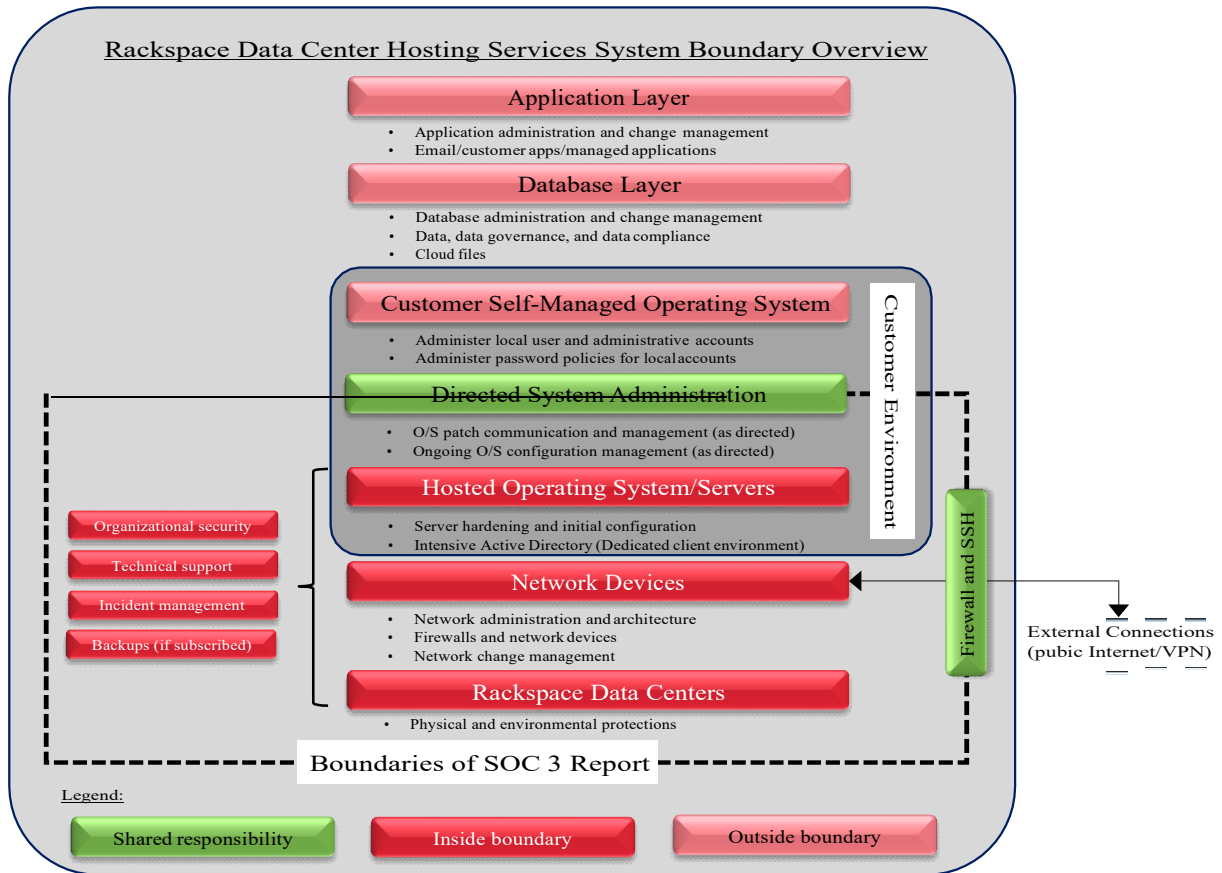
Data Center Hosting Services Boundaries and Scope of Report
This report includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the Data Center Hosting Services System at Rackspace.

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

The system boundaries relating to this SOC 3 report start at the edge/entry point of the network and extend through the corporate network domain and includes the dedicated infrastructure environment.

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

Rackspace Data Center Hosting Services System Boundary Overview

Application Layer
- Application administration and change management
- Email/customer apps/managed applications

Database Layer
- Database administration and change management
- Data, data governance, and data compliance
- Cloud files

Customer Self-Managed Operating System
- Administer local user and administrative accounts
- Administer password policies for local accounts

Directed System Administration
- O/S patch communication and management (as directed)
- Ongoing O/S configuration management (as directed)

Hosted Operating System/Servers
- Server hardening and initial configuration
- Intensive Active Directory (Dedicated client environment)

Organizational security
Technical support
Incident management
Backups (if subscribed)

Network Devices
- Network administration and architecture
- Firewalls and network devices
- Network change management

Rackspace Data Centers
- Physical and environmental protections

Customer Environment

Firewall and SSH

External Connections
(pubic Internet/VPN)

Boundaries of SOC 3 Report

Legend:
Shared responsibility | Inside boundary | Outside boundary

B. System Components

(1) Infrastructure

The boundaries for the data centers in-scope include both owned, operated, and leased data center facilities. This report covers the Data Center Hosting Services at the following data centers (in-scope data centers):

Data Center	Location	Ownership Type	Vendor
DFW2	Dallas, Texas	Operated	Not applicable
DFW3	Dallas, Texas	Operated	Not applicable
FRA1	Frankfurt, Germany	Leased	Digital Realty Trust
HKG1	Hong Kong, China	Leased	PCCW Solutions
IAD3	Ashburn, Virginia	Leased	Digital Realty Trust
IAD4	Ashburn, Virginia	Leased	Equinix Limited
LON3	London, United Kingdom	Owned	Not applicable
LON5	London, United Kingdom	Leased	Digital Realty Trust
ORD1	Chicago, Illinois	Leased	Digital Realty Trust
SYD2	Sydney, Australia	Leased	Digital Realty Trust
SYD4	Sydney, Australia	Leased	Equinix Limited

Rackspace owned or operated data centers are those for which Rackspace does not utilize a vendor for any services. For the leased data center facilities (FRA1, HKG1, IAD3, IAD4, LON5, ORD1, SYD2, and SYD4) Rackspace maintains direct monitoring controls, including annual risk assessments, a review of third-party reports, and periodic touchpoints with the operators of the data centers to provide coverage over the physical and environmental controls performed at those data centers.

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

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

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

(2) Software

Software systems are managed globally by Rackspace using consistent controls and processes. Rackspace utilizes a variety of software systems that support the Data Center Hosting Services System.

Operating Systems/Platforms

Rackspace supports a number of different operating systems as part of the Data Center Hosting Services System. Platforms within the system boundaries include:

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

Operational Support Tools

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

- Service management and asset management tools;
- System configuration management tools; and
- Patch management tools.

Authentication/Authorization Services & Isolation Mechanisms

In supporting both the Data Center Hosting Services System as well as providing support to Rackspace customers, Rackspace has implemented a series of tools that support authentication and authorization of individuals. Technologies within the system boundaries include:

- Directory services tools; and
- Authentication, authorization, and accounting tools for managing access to network components.

Security Tools

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

- Anti-virus/anti-malware;
- Intrusion Detection System; and
- Logging tools.

Performance Monitoring Tools

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

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

Other Tools and/or Services Supporting Infrastructure Components

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

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

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

- Managed Backup – a collection of servers in each data center utilized to provide data backup services for customers.

- Managed Storage – network attached storage in support of customers in virtualized environments as well as customers expanding storage requirements beyond their physical dedicated server offerings.

- Segment Support Patching –operating systems patching and update servers for supporting operating systems at the request of customers. Customers are responsible for all validation of these activities in line with their compliance requirements.

    ◻   Rackspace Virtual Infrastructure - includes all management components of the virtualized infrastructure hosting service.

(3) People

In order to meet its commitments and requirements as they relate to security and availability, Rackspace has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.

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.

The Rackspace Leadership Team actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

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

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

Employee competence is a key element of the control environment. Rackspace is committed to training and developing its employees. At least annually, the Human Resources Team/Management performs a review of key talent by individual and role to ensure that critical talent is retained and to ensure that the organizational structure is aligned in a way that will support achievement of the Company's objectives and strategies.

(4) Procedures

Policies and Procedures

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

and governance. The policies and procedures are a series of documents, which are used to describe the controls implemented within the Data Center Hosting Services System. The purpose of the policies and procedures are to describe the environment and define the practices performed on behalf of the customer. The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and Rackspace's commitments.

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

(5) Data

Data, as defined by Rackspace, constitutes the following:

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

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

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

ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Rackspace's service commitments and system requirements are included in the Managed Hosting Services Terms and Conditions which are available on Rackspace's website. Customers are provided and required to agree to the Terms and Conditions. The Terms and Conditions documents the contractual obligations of Rackspace Data Center Hosting Services and the customers using Rackspace's Data Center Hosting Services, including principal service commitments and system requirements. Any updates to the Terms and Conditions are communication to customers through the website and through the Customer Portal. In addition, Rackspace's service commitments and system requirements are communicated to internal users through Rackspace's intranet.

Only the principal service commitments and system requirements relevant to the applicable trust services criteria are within the boundaries of the system. The relevant service commitments and system requirements are included within the following sections of the Terms and Conditions:

4. Service Level Guaranties

    4.1 Network
    4.2 Infrastructure
    4.3 Hardware Repair or Replacement
    4.4 Replication Appliance
    4.5 Storage Devices
    4.8 Maintenance

11. Managed Backup

Additionally, the system description that reflects the boundaries of the Data Center Hosting Services system is available online for customers and prospective customers.