



*experience
fanatical
support®*

2009 Rackspace Hosting Description of Controls

Rackspace Compliance Department

Kiprian Miles
Vice President Information Services
Chief Security Officer

Rackspace Description of Controls

Company Overview

Rackspace Hosting began operations in December 1998 to provide managed web hosting services to small to medium sized businesses. Today, Rackspace services over 31,000 customers, including many Fortune 500 companies, in eight data centers worldwide. There are currently over 2,000 Rackspace employees (Rackers) around the world. Rackspace integrates the industry's best technologies and practices for each customer's specific need and delivers it as a service via the company's commitment to Fanatical Support®.

Hosting Services

Rackspace services a broad range of customers with diverse hosting needs and requirements. Rackspace has traditional, Cloud, and e-mail hosting segments to support their client's needs. The Intensive® segment supports clients who have increased needs by either transaction volume or complexity of environment. The Managed segment generally supports small- to medium-sized implementations. Rackspace has a third segment, called Platform, which serves clients that have significant in-house expertise and only require support around the physical infrastructure. Cloud Hosting is the newest division of Rackspace. Cloud serves clients scalable IT-enabled capabilities using Internet technologies. Mailtrust™ provides business e-mail hosting to companies of all sizes. Mailtrust offering includes Hosted Microsoft Exchange, Noteworthy® (POP, IMAP and Webmail), and Exchange Hybrids.

Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of management, the board of directors, and others 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 US, Inc. is internally organized into business units or "segments." They are, Managed, Platform, Cloud (Cloud Sites, Cloud Files, & Cloud Servers), Mailtrust and Intensive. There are seven global functions, which support these segments:

Engineering, Accounting & Finance, Legal, Employee Services, Sales & Marketing, Information Technology and Corporate Development/Strategy. These global functions have been established to provide capabilities to complement the segments, and to realize economies of scale and quality control. Each segment is led by a

segment leader. The leaders of the various global functions, the segment leaders, and 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 and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values of all Rackspace personnel. Rackspace technicians are staffed on a 24/7 basis to offer assistance with the installation and maintenance of various applications and to handle any critical system failures that may arise. Rackspace staffs its support teams and data center operations teams with technicians certified in various areas of expertise. Certifications held by Rackspace technicians include:

- Microsoft Certified Systems Engineer
- Microsoft Certified Professional
- Microsoft Certified Trainer
- Red Hat Certified Engineer
- Certified Information Systems Security Professional
- Certified Information Security Manager
- Cisco Certified Internetwork Expert
- Brocade Certified Fabric Professional
- Dell Certified Systems Expert
- Legato Certified Networker Administrator
- VMware Certified Engineers

Rackspace is also a Microsoft Gold Certified Partner and maintains a Microsoft Premier Services Agreement with Microsoft to provide vendor assistance and escalation of critical issues. In 2007, Rackspace was named the Microsoft Hosting Provider of the Year. The Rackspace network is a Cisco Powered Network and Rackspace is a Cisco Service Provider Partner. The Company maintains a Cisco support and maintenance contract, which includes software upgrades, hardware support and replacement, and support from the Cisco Technical Assistance Center (TAC).

Commitment to Competence

The competence of employees is a key element of the control environment. 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 evidence of integrity and ethical behavior. Rackspace's commitment to the training and development of its employees is demonstrated by the creation of a dedicated training organization called Rackspace University. The training and development path is co-managed by each employee and his or her manager. All training is coordinated through Rackspace University. The process entails the development of specific, quantifiable objectives for the coming performance year, periodic discussions of progress in meeting those objectives, and a semi-annual formal review of the employee's overall performance in the current position as well as career development discussions to help prepare the individual for advancement.

Rackspace management has implemented a division of roles and responsibilities, which provides adequate segregation of duties. The primary mechanisms used to enforce segregation of duties are the physical and logical access controls in place at Rackspace to control access to customer data and assets. Physical access restrictions for personnel are enforced with the use of a color-coded ID badge system, proximity access cards, and biometric access devices. Logical access to core networking equipment and customer resources requires password access and is granted only to those personnel in roles that require such access.

Risk Assessment Process

An entity's risk assessment process is its identification, analysis, and management of risks relevant to the preparation of its financial statements and to user organizations. Rackspace recognizes that risk management is a critical component of its operations that helps to verify that customer assets are properly maintained. Rackspace incorporates risk management throughout its processes at both the corporate and segment levels.

The management of each segment is responsible for implementing procedures to identify the risks inherent in the unit's operations and for implementing procedures to monitor and mitigate the risks. The foundation of this process is management's knowledge of its operations, its close working relationship with its customers and vendors, and its understanding of the industry in which it operates. Managers discuss and resolve issues as they arise within their areas, and monitor and adjust the control processes for which they are responsible on an as-needed basis. This is done both informally and formally through regularly scheduled meetings. Rackspace manages risks on an ongoing basis through a formal project management process. Rackspace has an overall strategic plan that is presented to the Board of Directors. This strategic plan is then separated into specific segment plans that are designed to

operationalize what is expected of the segments in order to support Rackspace's overall objectives.

Rackspace uses a number of different procedures to manage its business risks. Contracts and amendments with vendors and customers are reviewed by Rackspace's in house legal counsel. Finally, monitoring of performance against existing contracts with vendors and customers is a critical function performed by all of Rackspace's segments.

Information and Communication

To help align Rackspace business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. Management across all functional areas participates 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.

On a monthly basis, a Directors' and Officers' report is provided to Rackspace management that summarizes the performance statistics of the various segments within the Company, including but not limited to, key financial data, employee headcount information, inventory and recycling rates, and goal attainment reports. On a real-time basis, Rackspace personnel can access key performance metrics using the Rackspace Data Warehouse Corporate Reporting Portal. Financial performance, as well as key corporate and department goals, are presented to all Rackspace employees during quarterly, company-wide Open Book meetings.

Rackspace has implemented a security awareness notification email list through which employees are provided ongoing guidance and best practice information on securing data, assets, and other sensitive information. Changes and updates to security policy are communicated to all employees through company-wide email and through the Rackspace Risk Management Department. New employees are briefed on Rackspace security policy during employee orientation and each employee signs a security acknowledgement form and confidentiality agreement.

Control Activities

Control activities are the policies and procedures that help verify that management directives are carried out. They help verify that necessary actions are taken to address risks that may jeopardize the achievement of the entity's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels. Rackspace's management team is responsible for directing and controlling operations, and for establishing, communicating, and monitoring control policies and procedures. Rackspace maintains sound internal controls and holds high expectations for the integrity and ethical values of all Rackspace personnel.

Organizational values and behavioral standards are communicated to all personnel, via Rackspace's Intranet and the Rackspace employee handbook and are reinforced in company communications. Rackspace's executive officers evaluate actual performance against budgeted performance on a quarterly basis. In addition, segment heads perform a detailed review of quarterly performance against submitted budgets for their department.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. To complement these measures, all exceptions to normal or scheduled processing related to hardware, software, or procedural problems are logged, reported, and tracked until resolved. Key reports are reviewed by management to help verify that appropriate action is taken.

Rackspace's management and supervisory personnel monitor the quality of internal control performance as a routine part of ongoing activities. Rackspace has implemented a series of management reports that measure the results of providing a robust, scalable, and secure infrastructure for client organizations. Performance metric reports include data on actual system availability compared with established service level goals and standards. Performance metric reports are reviewed by appropriate levels of management, and action is taken when necessary.

General Computer Controls

Human Resources and Training

Rackspace is composed of separate organizational elements, with an adequate segregation of duties maintained between and within the organizational elements, to facilitate an efficient execution of business processes. Management has implemented a division of roles and responsibilities that limits the possibility for a single individual to subvert critical processes. Policies and procedures are in place to ensure that personnel perform only those duties related to their positions. Management ensures that position descriptions used to delineate employee responsibilities and authority are established and updated as needed.

Management ensures that US employees are subjected to a background check, including social security, criminal record and educational background verification. The UK employees undergo a Legal Right to live and work in the UK check, employment verification, education background verification (where applicable), and depending on the position, trade, criminal and/or credit verification.

New employees at Rackspace Corporate locations are required to attend Rookie Orientation, a new hire program presented by Rackspace University, which teaches Rackspace culture, Rackspace structure, and selective policies and departmental functions. Rackspace University also conducts a Support Fundamentals class after Rookie Orientation for new Rackers in customer facing queue-related roles. Product training is developed and scheduled based on the product release schedule, and these classes are offered as necessary. Management training is provided for Managers who are hired or promoted that have direct reports.

Information Security

Rackspace implements Information Security best practices to protect the confidentiality and integrity of customer and company data systems. A Security Awareness program communicates security expectations to Rackspace workforce during the initial Security training at new employee orientation. Quarterly Security Awareness bulletins also support the Security awareness program. All visitors are required to sign in via a visitor log. Building Operations, Security or Data Center Management review and approve visitor access and issue visitor badges for identification purposes before access is granted to any non-Rackspace employee. For our facilities in London, in lieu of sign off sheets, an email of visitor logs is reviewed by the Data Center Manager and emailed to Rackspace Corporate Security. Controlled building access and secure access to specific areas are ensured through the administration of proximity cards. An Incident Response Process has been instituted to respond to and document security incidents.

Physical Data Center Access and Environmental Controls

Rackspace operates eight data centers hosting customers; three located in Texas, two located in Virginia and three international data centers in London, England and one in Hong Kong, China. Each data center is a single-purpose facility engineered to address security and network redundancy, enabling Rackspace to offer high availability to its customers. The below description of the data center's environmental and physical access controls includes controls that are common to all data centers in scope; however, certain data centers may have additional controls to supplement those described in this report.

Data Center Facilities

Rackspace data centers feature redundant HVAC (Heating Ventilation Air Conditioning) units, which provide consistent temperature and humidity within the raised floor area. HVAC systems are inspected regularly and air filters are changed periodically. Redundant lines of communication to telecommunication providers provide Rackspace customers with failover communication paths in the event of data communications interruption.

Data centers are equipped with sensors, including smoke detectors, and floor water detectors, to detect environmental hazards. The data centers are also equipped with raised flooring to protect hardware and communications equipment from water

damage. Data centers are equipped with fire detection and suppression systems, fire extinguishers, and fire detection systems. Fire detection systems, sprinkler systems and chemical fire extinguishers are inspected at least annually.

Data center and office facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The UPS power subsystem is N+1 redundant with instantaneous failover in the event of a primary UPS failure. The UPS systems are inspected on a monthly basis. Data center and office facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. Generators are regularly tested and maintained to provide assurance of appropriate operability in the event of an emergency. These tests occur on a monthly basis. At the data center level, Rackspace personnel are on duty 24 hours a day, 7 days a week at all of Rackspace's data center facilities.

Data Center Physical Access

Rackspace personnel are required to display their identity badges at all times when onsite at Rackspace data centers and non-data center facilities. Two-factor authentication is required to gain access to the data center facilities. Electromechanical locks are controlled by biometric authentication (hand geometry scanner) and key-card/badge. Only authorized Rackspace personnel have access to data center facilities. Closed circuit video surveillance has been installed at all entrance points on the interior and exterior of the buildings housing data centers.

Infrastructure Maintenance and Change Management

Overview of Shared Infrastructure

Rackspace shared infrastructure represents any component of the communications network or physical environment that is not customer specific. Shared infrastructure is utilized by more than one Rackspace customer to gain economies of scale for appropriate types of equipment. Examples include core routers and switches, SAN fabric, backup infrastructure, Internet backbone connections, etc. Customer specific communications equipment represents the demarcation of shared infrastructure, which would follow the process and controls described below.

Project Initiation

All infrastructure changes follow a structured change methodology. An engineering maintenance controller coordinates all changes to the Rackspace infrastructure to ensure the involvement of appropriate technical resources in the design and delivery of these changes, adequate testing, planning and documentation. Projects impacting shared infrastructure can only be initiated by owners of the impacted infrastructure component. To the extent that the change impacts other stakeholders, other appropriate infrastructure owners are involved as needed by the engineering maintenance controller.

All planned infrastructure changes must be submitted to the Service Assurance committee and approved by the committee prior to the scheduled maintenance. For all medium impact changes, Engineering Management authorizes the change prior to submission to the Service Assurance Committee (SA). For low impact changes, the SA does have the ability to disallow the change to proceed; however, for low impact changes the SA time allotted during the meeting is not large. Most of the low impact changes are routine maintenance where the SA and the Company as a whole are aware of the risks and mitigating controls required by the change.

Once the initiator of the change has prepared a preliminary project plan, the engineering maintenance controller works with the initiator to verify that the document has complete and relevant information. It can then be presented to the VP of Engineering and/or the SA. From change inception to finalization, the engineering maintenance controller continues to work with all relevant stakeholders to provide assurance that all potential interdependencies have been considered and appropriately addressed.

If implementation of scheduled infrastructure software and hardware changes are known to have a possibility of disruption of service, customers are provided information on the effects of the changes to their operations, and are given time to schedule appropriate actions. All correspondence with the customer regarding the planned infrastructure changes are documented in a CORE ticket. The creation of a CORE ticket generates an e-mail notification to the designated customer contact(s).

Testing

All infrastructure changes undergo appropriate levels of testing. Testing is performed once the test plan has been developed by the project initiator and vetted through relevant technical leads, including the engineering maintenance controller, and all necessary equipment has been obtained. Typically, testing is performed in a segregated test lab on the Rackspace campus. The level of testing performed is dependent on the nature of the project being implemented, but follows the vendor's recommended test strategy, when applicable.

Implementation

When the engineering maintenance controller agrees with the initiator that all appropriate authorizations and approvals have been obtained and that an appropriate level of testing has been successfully performed, the change is then approved for migration into the production environment. Maintenance activities are scheduled on the SA maintenance calendar to avoid conflicts and to provide for advanced planning and notification to customers, if necessary.

A post maintenance communication email highlighting the changes that took place and the results of those changes is sent to the Rackspace staff informing them when the maintenance activity is complete. After the maintenance is completed, an analysis of any unexpected issues or failures that arose during the process is performed and reported to the SA. The Customer Care Team is responsible for

handling of the Rackspace Customer's environment. The Customer Care Teams review and approve the changes prior to changes being placed into the production environment.

Logical Access

Rackspace customers retain full administrative rights and control of their Rackspace implementation. The customer is therefore considered the primary system administrator of their environment. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment. Customers have full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. Rackspace customers may make changes to their servers as needed, including uploading content, configuring software and security settings, adding or removing local users and changing passwords.

Rackspace User Administration

Rackspace policies require users to be specifically authorized to access information and system resources, except for certain specified data that is available to all employees. The Information Services (IS) Department is responsible for security administration functions, including assigning/deleting users to internal Rackspace system resources. The technical leads within the Linux, Active Directory and Windows 2003 environments are responsible for administering and initiating access rules for their respective environments. Rackspace has logically separate networks for all internal traffic, resulting in Rackspace administration of customer environments being performed from specified networks within the Rackspace environment. All Rackspace user access requests follow a documented, formal process and must be approved by a manager or supervisor who owns the tool or infrastructure component for which the request is being made. Upon termination from Rackspace, employee access is removed from Active Directory.

When an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts IS. IS will then change the transferred employee's access rights to verify that they are commensurate with the employee's new position. The Human Resources Department generates a listing of all employee terminations on a weekly basis and forwards this listing to Corporate Security so that the employee's access can be disabled or removed from the appropriate systems. In addition, the manager of the terminated employee may also inform IS of the need to revoke access from a user account.

Network Management

Dedicated customer Virtual networks (VLAN) are used to logically segment customers on the Rackspace network into different broadcast domains so that packets are only switched between ports that are designated on the same VLAN. Firewalls are configured with Access Control Lists (ACL), which prevent access to private internal IPs and deny access to all non-Administrative ports. All non-

administrative ports are closed by default unless specifically requested by the customer. Administrative activity by Rackspace on customer servers is limited to specific internal Rackspace IP address ranges. Additionally, the customer may specify IP address ranges to be used to tightly restrict customer remote administration. Routers are configured to prevent Denial of Service (DoS) attacks through the use of anti-spoofing Access Control Listings (ACLs).

TACACS+ is an industry standard network device access control system. Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in TACACS+ software. Processes are in place to review the TACACS+ access lists on a quarterly basis to verify those users on the list still require access. Any discrepancies found are corrected immediately.

Backup of Programs and Data Files

Rackspace offers backups of data on customer servers using backup utility software. Customer servers are logically segmented, through the use of a dedicated VLAN on the network for communication to the backup servers. Rackspace works with customers to establish the appropriate backup schedule and what portions of the customer's implementation require backup. Prior to finalizing backup configuration, an initial test backup is run in order to determine that backups will run properly.

The back-up utility software performs backups according to the predetermined schedule determined by the customer and tracks all tapes within the automated tape library using bar codes. Automatic testing of the tape media is performed by the backup software at various times to verify that tape media are suitable for use. All backup failures are logged by the backup utility software. The MyRackspace® customer portal displays a report with the most recent backup success/failure status, including the volume of backed up information.

An automated tape library is utilized to track backup tapes. All tapes are bar coded and scanned by the library using the backup utility software. The most current full backup of customer data is stored on site in the tape library. Backup media is rotated off-site according to the media rotation schedule purchased by customer. Media is stored at a secure, offsite storage facility and transported in a locked container. Tapes stored offsite are maintained by a records storage vendor and transported to offsite facilities in locked containers. Backup tapes are securely destroyed when their useful life expires. The destruction process physically destroys the media to prevent retrieval of data.