Cloud Security

Security & Certification for Cloud Solutions

Version 1.0

This document details the security facilities and certification for cloud based solutions

Contents

Overview

This document details the security and compliance for our cloud based solutions which are hosted through Rackspace who have many global data centres across 3 continents which are ISAE 3402 Type II SOC 1 Audited and uses the latest in data centre technology to help deliver a secure environment for our customers. The London data centre has 28GB/s aggregate IP transit and over 74,000 ft2.

Certification

ISO 27001:2005 (Information Security)

Our UK and Hong Kong data centres are certified to the international standard for information security, ISO 27001. This standard provides a framework for managing a business' security responsibilities and provides external assurance for customers as to the scope and scale of our secure environment via our Business Security Management System.

Since 2009 our system has provided the foundation for an integrated and sustainable security model working in tandem with our other security controls such as PCI-DSS. It is subject to on-going external assessment by our certification body, Certification Europe with a full re-assessment every three years.

ISAE 3402 Type II Service Organization Control

We utilise this globally recognised standard for reporting on service organisation controls to demonstrate that selected processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing company (service auditor) for our managed hosting customers, cloud servers & cloud files customers and all our data centres. The examination includes controls relating to security monitoring, change management, service delivery, support services, back-up, environmental controls, logical and physical access and provides a detailed description of our controls and the effectiveness of those controls.

We have completed an examination in conformity with the International Standard for Assurance Engagements (ISAE) No 3402 Type II Service Organization Control (SOC) 1 which is repeated on an annual basis.

We recognise the needs of our global customers and has worked with the service auditor to have the report issued with a joint opinion that satisfies the requirements of both the ISAE 3402 and the SSAE 16 (created by AICPA (American Institute of Certified Public Accountants) for use in the US mirroring ISAE 3402)).

PCI Data Security Standard (DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard defined by the Payment Card Industry Security Standards Council (PCI SSC).

The purpose of the standard is to reduce credit card fraud. This is achieved through increased controls around data and its exposure to compromise. The standard applies to all organizations which process, store, or transmit cardholder information. In June 2009, Rackspace was approved by Visa as a Compliant Level 1 Payment Card Industry (PCI) Service Provider and continues to be audited annually to ensure continued adherence to the requirements of the standard.

ISO 14001:2004 (Environmental Management) and BS OHSAS 18001:2007 (Occupational Health & Safety)

We take environmental and workplace responsibilities seriously, from ensuring we provide a safe and healthy working environment for our team through to our commitments to the wider world: legally and morally.

In support of this, our UK data centres and office are certified to both the international environmental management standard, ISO 14001, which provides a framework for managing our environmental responsibilities, including energy and waste management, and BS OHS 18001 for our commitment to workplace wellbeing.

Both certifications are subject to on-going external assessment by our certification body, BSI (British Standards Institution), with a full re-assessment every three years.

Our ISO 14001 certificate number is EMS 581182 and our BS OHS 18001 is numbered OHS 587454.

Security and Compliance

Physical Security

Physical Security includes locking down and logging all physical access to our data centres.

- Data centre access is limited to only authorised personnel
- Badges and biometric scanning for controlled data centre access
- Security camera monitoring at all data centre locations
- Access and video surveillance log retention
- 24x7 onsite staff provides additional protection against unauthorised entry
- Unmarked facilities to help maintain low profile
- Physical security audited by independent firms annually

Operations security

Operational security involves creating business processes and policies that follow security best practices to limit access to confidential information and maintain tight security over time.

- Data centre access is limited to only authorised personnel
- ISO 27001/2 based policies, reviewed at least annually
- Documented infrastructure change management procedures
- Secure document and media destruction
- Incident management function
- Business continuity plan focused on availability of infrastructure
- Independent reviews performed by third parties
- Continuous monitoring and improvement of security programme

Network infrastructure

Network infrastructure provides the availability guarantees backed by aggressive SLAs.

- High-performance bandwidth provided by multiple network providers
- Elimination of single points of failure throughout shared network infrastructure
- Cables properly trunked and secured
- Proactive network management methodology monitors network route efficiency
- Real-time topology and configuration improvements to adjust for anomalies
- Network uptime backed by Service Level Agreements
- Network management performed by authorised personnel only

SAN and Hard Disks

Our servers are connected to an EMC VMAX SAN with multiple tenants, which are logically segregated, so no other customer has access to your data.

This array uses data at rest (D@RE) as a way to encrypt your data. D@RE provides encryption on the back end using SAS I/O modules that incorporate XTS-AES 256-bit-data-at-rest-encryption. These modules encrypt and decrypt data as it is being written to or read from a physical drive.

All configured drives are encrypted, including data drives, spares, and drives with no provisioned volumes. In addition, all cached user data stored in Power Vault is also encrypted.

Data at rest incorporates RSA embedded Data Protection Manager (eDPM) for key management. With D@RE, keys are self-managed, and there is no need to replicate keys across volume snapshots or remote sites.

RSA Embedded Key Manager provides a separate, unique DEK for each drive in the array, including spare drives.

The encryption on SAN is XTS-AES 256-bit-data-at-rest-encryption and is FIPS 140-2 certified.

The SAN array has an off-site copy maintained in on a similar EMC VMAX SAN which is held at a separate UK location. Please see appendix with Rackspace locations and facilities.

Environmental controls

Environmental controls implemented to help mitigate the risk of service interruption caused by fires, floods, and other forms of natural disasters.

- Dual power paths into facilities
- Uninterruptable power supplies (minimum N+1)
- Diesel generators (minimum N+1)
- Service agreements with fuel suppliers
- HVAC (minimum N+1)
- VESDA / fire suppression
- Flood detection
- Continuous facility monitoring

Human resources

Human resources provides employees with an education curriculum to help ensure that they understand their roles and responsibilities as they relate to information security.

- Background screening performed on employees with access to customer accounts
- Employees are required to sign non-disclosure and confidentiality agreements
- Employees undergo mandatory security awareness training upon employment and annually thereafter

Security organisation

Security organisation includes establishing a Global Security Services team tasked with managing operational risk, by executing an information management framework based on the internationally recognized ISO 27001 Standard.

- Security management responsibilities assigned to Global Security Services
- Chief Security Officer with oversight of Security Operations and Governance, Risk, and Compliance activities
- Direct involvement with Incident Management, Change Management, and Business Continuity

Rackspace Locations and Facilities

LON 3 – SLOUGH

Facility & Security

- Raised Flooring: 5,000 sq m
- 15 MVA Total Utility Power
- Manned 24x7x365
- Biometric Scanners
- Video Surveillance
- Alarm System
- Key Card Access Required
- Laser Based Smoke Detection

Connectivity & Infrastructure

- Multiple Tier-1 Service Providers
- 10-Gigabit Ethernet Per Carrier
- Redundant Cisco 3-Tier LAN Architecture
- 8 Carriers Providing Fiber Based Connectivity to Site
- Redundant Cisco & ARISTA Routers
- BGP Multipath Route Optimization
- Cisco Switches for Aggregation

Power & Cooling

- 250 kW UPS Power Capacity
- N+1 Redundancy
- Diesel-Powered Generators with 2MW Capacity each
- 10,000 Litre Fuel Tanks
- Over 3,000 Tons of Cooling
- Capacity, N+3 Redundancy
- Double Interlocked Dry Pipe Pre-Action Sprinkler System

100% Renewable Energy

LON 5 – CRAWLEY, WEST SUSSEX

Facility & Security

- Data Hall Flooring: 6,606 sq m
- 18 MVA Total Utility Power
- Manned 24x7x365
- Biometric Scanners
- Video Surveillance
- Alarm System
- Key Card Access Required
- Laser Based Smoke Detection

Connectivity & Infrastructure

- Multiple Tier-1 Service Providers
- 10-Gigabit Ethernet Per Carrier
- Redundant Cisco 3-Tier LAN Architecture
- 7 Carriers Providing Fibre Based Connectivity to Site
- Redundant Cisco & ARISTA Routers
- BGP Multipath Route Optimization
- Cisco Switches for Aggregation Distribution & Access Layer

Power & Cooling

- 12 MVA UPS Power Capacity
- N+1 Redundancy
- Diesel-Powered Generators w/ 1.6875 MW Capacity each
- 50,050 Litre Fuel Tanks
- Over 106 Tons of Cooling Capacity, N+2 Redundancy
- Double Interlocked Dry Pipe Pre-Action Sprinkler System

100% Renewable Energy

LON 8 - LONDON

Facility & Security

- Raised Flooring: 7,561 sq m
- 17 MVA Total Utility Power
- Manned 24x7x365
- Biometric Scanners
- Video Surveillance
- Alarm System
- Key Card Access Required
- Laser Based Smoke Detection

Connectivity & Infrastructure

- One Tier-2 Service Providers
- 10-Gigabit Ethernet Per Carrier
- Redundant Cisco 2-Tier LAN
- Architecture
- 2 Carriers Providing Fiber Based Connectivity to Site
- Redundant Cisco & ARISTA Routers
- Cisco Switches for Access Layer

Power & Cooling

- 423 kW UPS Power Capacity
- N+1 Redundancy
- Diesel-Powered Generators with 3,800 kVA Capacity each
- Two Plants of 3x900kWr Air-cooled Package Chillers with 3,600kWr Total, N+1 Redundancy
- Double Interlocked Dry Pipe Pre-Action Sprinkler System

ALL SITES

Standards & Compliance

Rackspace adheres to a broad range of information and security certifications & standards including:

- SSAE18 SOC1, SOC2, SOC3
- PCI DSS
- ISO27001
- ISO14001
- ISO9001

Accessibility & Monitoring

- Customers Retain Admin Control of Leased Servers
- Rackspace Retains Control of Networking Hardware
- Console Access Provided via SSH over VPN Centralised Facility
- Monitoring & Management System