ORA Web-Systems Data Delivery and Security

Occupational Research and Assessment, Inc. (ORA) uses Rackspace as its data center. Rackspace was established in 1998 with headquarters near San Antonio, TX and data centers in multiple locations. Rackspace is an enterprise-level hosting service to businesses of all sizes worldwide. Rackspace integrates the industry's best technologies and delivers it as either "managed" or "unmanaged" data center service. The US Department of Justice (USDOJ), National Institute of Justice (NIJ) uses Rackspace for hosting the National Missing and Unidentified Persons System (NamUs). Full data back-ups are performed every 24 hours.

The following is an outlined breakdown of the data centers security and infrastructure supplied by Rackspace and available at www.rackspace.com:

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

- Data center access is limited to only authorized personnel
- Badges and biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- Access and video surveillance log retention
- 24x7 onsite staff provides additional protection against unauthorized 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.

- 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 program

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 authorized personnel only

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 Rackspace 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 Organization
Security Organization 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 Security Assessments and Compliance
Rackspace maintains various certifications to assist you in verifying the security policies and processes that Rackspace has in place for the environment of the hosted infrastructure. Rackspace has been assessed and holds validation for the following compliance frameworks:

- ISO 27001
- SSAE 16 and ISAE 3402 (Previously SAS 70 Type II)
- PCI DSS
- SOC 2
- SOC 3
- Safe Harbor (export.gov)

NOTE: Rackspace certifications do not make your office compliant with your specific regulatory and compliance requirements.

ISO 27001
ISO 27001 is an international information security management standard. It defines how to design, implement, and maintain an Information Security Management System (ISMS). The Rackspace ISO 27001 certified ISMS is an iterative management system that helps ensure that our security policies and processes are effective in mitigating identified risks. Specifically, the ISMS at Rackspace certifies the management of information security in the operations of our data center facilities.

SSAE 16 and ISAE 3402

SSAE 16 (Statement on Standards for Attestation Engagements No. 16) is an internationally recognized auditing standard used to assess the controls in place at a third-party service organization. An SSAE 16 Type II audit, along with the completed audit report, provide customers of companies like Rackspace with externally validated and unbiased information about the nature and effectiveness of the controls in place at our operations.

ISAE 3402 is the international version of SSAE 16. Together they replace the SAS 70 auditing standard.

The global Rackspace Type II SOC1 report can be used to satisfy requirements under both the SSAE 16 and ISAE 3402 standards. This report contains a description of the controls we have in place and the auditor's informed opinion of how effective the controls were during the audit period. The audit period for Rackspace extends from October 1st to September 30th each year.

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) is a security standard that provides an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate responses to security incidents. A Qualified Security Assessor (QSA) validates Rackspace as being a PCI DSS Level 1 Service Provider. The QSA validation of our compliance to the PCI DSS covers:

- Physical security for Rackspace data centers located in:
- United Kingdom
- Hong Kong
- United States
- Network infrastructure (routers and switches)
- Rackspace employee access to network devices

Please note that simply hosting a solution with Rackspace **does not** make you PCI-DSS compliant. However, outsourcing hosting services to a PCI DSS validated Level 1 Service Provider can greatly reduce the scope and complexity of your compliance efforts. Rackspace can provide products, services and an extensive solution partner network that can help satisfy many of your PCI-DSS requirements.

SOC 2

- Reports on controls at a service organization relevant to Security, Availability, Privacy, Confidentiality and Processing.
- SOC 2 engagements use the predefined criteria in Trust Services Principles, Criteria and Illustrations, as well as the requirements and guidance in AT Section 101, Attest
- Engagements, of SSAEs.
- These reports are intended to meet the needs of a hosting provider customer that needs to understand the internal controls at a service organization.
- SOC 2 framework is a reporting option specifically designed for entities such as data centers, IT managed services, software as a service (SaaS) vendors, and many other technology and cloud computing based businesses.
- A Type 2 report also includes the service auditor's opinion on whether the controls were operating effectively and describes tests of the controls performed by the service auditor to form that opinion and the results of those tests.

SOC 3

Due to the restrictions of distribution to current and potential customers for the SOC 1 and SOC 2 reports, Rackspace has obtained a SOC 3 report. The difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report contains a detailed description of the service auditor's tests of controls and results of those tests as well as the auditor's opinion on the description of the service organization's system. A SOC 3 report provides only the auditor's report on whether the system achieved the trust services criteria. There is no description of tests and results or opinion on the description of the system.