WorkItem.com®
GMI Management Operating System

Information Security

Frequently Asked Questions
January 1, 2017

Contents

1.0 Security Oversight and Governance

Ref.	Sub-Category	Question	Response
1.1.1	**Security Planning**	Do you have a documented information security policy and procedures?	Yes - See accompanying Information Security Policies and Procedures.
1.1.2		Do you periodically review policies and how frequently does that occur and describe who approves them?	Reviewed and updated annually, and approved by the CEO.
1.1.3		Describe your Data Loss Prevention Program (DLP) and the specific controls.	Data at rest is encrypted and production access is restricted. Logs are available to identify activities performed by all users. If a cybersecurity incident were to occur, we would bring in a specialized security consulting team to support us.
1.2.1	**Security Procedures**	Do you have documented procedures in place for critical functions and responsibilities?	Yes.
1.2.2		Do your security policy and procedures clearly define information security responsibilities for all employees and contractors?	Yes.
1.2.3		Have your employees and contractors who will be handling data been trained in information security safeguards?	Yes.
1.2.4		Do you have an employee and/or contractor hiring and termination process in place?	Yes.
1.2.5		Do your employees and contractors sign a non-disclosure agreement stating they will keep information obtained as part of their employment confidential?	Yes.

Ref.	Sub-Category	Question	Response
1.2.6		Are customers permitted to perform technical security assessments within your environment?	Yes, but with appropriate notice and at customer's expense.
1.2.7		Do you currently have insurance policies to protect against Cyber Threats, Business Interruption, etc.?	Yes.
1.3.1	**Security Awareness**	Please describe the security awareness program that you have in place for your employees and third parties.	Staff security awareness programs include comprehensive quarterly updates.
1.4.1	**Incident Response**	Please describe the Incident response process in the event that a security incident was to occur within your organization.	Please refer to the accompanying Incident Response Plan.
1.4.2		Do you have a documented and tested incident response plan to include identification, containment, eradication, and recovery of incidents?	Yes - See accompanying Incident Response Plan.
1.4.3		Do you have a process in place for notifications in the event of a security incident within your organization?	Yes - See accompanying Incident Response Plan.
1.5.1	**Audit and Risk Management**	Do you have an Independent Audit, Risk Management, and Information Security Function?	Yes, for Information Security and Risk Management. While there is no independent audit function, over the years we have been reviewed by clients' auditors (who have paid for the audits).
1.5.2		Are your operational controls independently tested on a periodic basis by either an internal and external auditor?	Controls have been independently tested, but not on a regular basis.
1.5.3		Please describe your risk management program or processes.	Risk management is embedded in each of our core processes. Risk probability and impact are assessed throughout the lifecycle, and remedial actions are taken as appropriate.

2.0 Data Management

Ref.	Sub-Category	Question	Response
2.1.1	**Data Retention**	Please provide information on the backup and the retention of data.	Backup and retention follow Rackspace standards.
2.1.2		What is the method to obtain the data stored in your system if you were to go out of business, or if we choose to discontinue use of the solution in favor of another system?	The application includes a feature that allows the client to download their data as an archival zip file.
2.2.1	**Data Disposal**	Are security procedures followed for the decommissioning and/or destruction of equipment and storage media which once held customers' data?	Client data is held on hardware resources used by multiple tenants. Data destruction involves deletion of the tenant database and not destruction of equipment or physical storage media. Offsite backups are destroyed when their rotation is finished, based on standard Rackspace procedures.
2.2.2		Do you have a data retention and disposal policy? Is storage of personally identifiable information (PII) kept to a minimum and the storage amount and retention time limited to that which is required for business?	Data is retained for as long as the client is active and using the product. Old data can be disposed of by the client, if desired. Our applications do not currently process or store any PII.
2.3.1	**Data Storage**	Do you use encryption to protect your workstations?	Yes.
2.3.2		Do you encrypt sensitive data at rest?	Yes - SQL Server 2012 encryption. See also 1.1.3.
2.3.3		Is data encrypted on backup media?	Yes.
2.3.4		Do the provider's administrators have access to view the customer's data in clear text? Are there role-based processes in place to ensure that only the appropriate individuals within the service provider's organization will have access to customer data?	Yes.

Ref.	Sub-Category	Question	Response
2.4.1	**Database Administration**	Please provide information on the backend database that this application utilizes. Please describe the type and the version of the database.	SQL Server 2012 Enterprise edition is used.
2.4.2		Have the default admin accounts such as system administrator (sa) account been renamed and has the password on the default accounts been changed?	Yes.
2.4.3		Do you have a process in place to scan the database for known vulnerabilities?	Yes, the database is monitored and scanned on a regular basis.
2.4.4		Do you have logging and monitoring of the databases? Are the database logs sent to the SIEM and what monitoring is in place?	Rackspace provides monitoring of the databases via the Alert Logic Threat Manager and Active Watch solutions, which include custom network Intrusion Detection System (IDS) tools, internal/external vulnerability scanning, and security information and event management (SIEM), and we receive alerts regarding any potential issues.
2.5.1	**Data Segregation**	Please provide information on how data is segregated from other tenants.	Each tenant has a physically separate SQL Server database.
2.5.2		How do you segregate between Production and Test? Will Customers' production data also reside in the test environment?	Separate servers are used. Production data is not used in the test environment.
2.5.3		If multi-tenant, what steps have been taken to secure data from being accessed from other tenants?	Each tenant has a physically separate SQL Server database. Each web request is associated with a tenant and is not able to access any other tenant data.
2.5.4		Is data encrypted over the service provider's internal network?	Yes.

3.0 Application Management

Ref.	Sub-Category	Question	Response
3.1.1	**Application Development**	Do you have separate development, test, and production environments?	Yes.
3.1.2		Are segregation of responsibilities maintained between the production and the test environment?	Yes. We segregate testing versus production data, use separate computing environments, and have Quality Assurance done separately from coding. Also, our computer operations are segregated by the fact that they are performed by Rackspace.
3.1.3		Is version control utilized during the application development process?	Yes.
3.1.4		Please describe your application development methodology/SDLC Process.	We employ an agile SDLC process methodology wherein a combination of iterative and incremental process models focuses on rapid delivery of high-quality, working software products and documentation.
3.1.5		Please describe how application security testing is a part of the product life cycle development?	We use a code migration process, facilitated by a revision control system, which culminates in point-in-time software builds. Changes promoted to the production code thread require additional, independent verification. Releases of production builds are driven via an automated deployment tool.
3.1.6		Are controls over the source code library maintained?	Yes
3.1.7		Do your developers receive secure coding training?	Yes
3.1.8		Please describe the secure code review process.	Our secure code review process relies on the results of our vulnerability scans. From these, we prioritize and mitigate any issues during the development process.

Ref.	Sub-Category	Question	Response
3.2.1	**Application Enhancements, Patching, and Upgrades**	How often are new releases introduced?	Typically, quarterly.
3.2.2		How closely is customer feedback considered in upgrade plans?	Customer input is essential to the development of new and upgraded functionality. As a SaaS application, all tenant instances are upgraded at the same time according to a published schedule.
3.2.3		How often do program updates go out and do you notify customers?	Quarterly. Yes, customers are notified.
3.2.4		What is the turnaround time for getting "bugs" fixed? How do you communicate your response to zero day vulnerabilities (e.g., POODLE)?	Bugs are prioritized according to their severity and impact to the customer. Critical bugs are given the highest priority and worked until fixed. Customers are notified via email of our response to all critical vulnerabilities. Non-critical fixes are reported via release notes.
3.2.5		Please describe your patching cycle within the application.	Where possible, we will not perform patching, waiting until the next release for such fixes. It is very rare for us to patch. In the event of a critical problem impacting all tenants, we would implement a fix ASAP during a time with minimal impact.
3.2.6		What is the policy for updating the underlying platform and how are release notes shared?	Enhancements and bug fixes are incorporated in a software release which is applied to all tenants within a maintenance window. All software changes are documented in release notes that can be accessed within the application.

Ref.	Sub-Category	Question	Response
3.3.1	**Application Reporting**	Please describe the types of reports available within the application, specifically in the following areas: - User Access Rights - User Privileges - Changes within the application - Changes within user accounts - User and Admin activity - Failed login attempts	All of these application-related security reports are available and restricted to tenants' administrators. The reports can be exported to Excel for further analysis.

4.0 Application Security

Ref.	Sub-Category	Question	Response
4.1.1	**Application Controls**	Does the application have built-in roles and do you have the logic built such that certain roles cannot be combined together?	Roles are represented in our workflow, and users are subject to certain restrictions (e.g., a single user is not allowed to participate within multiple worksteps). Each workstep's eligible participants can be further restricted to members of specific user groups.
4.1.2		What transaction security or fraud controls are built in to the application?	The application is not used for processing actual financial transactions.
4.1.3		What type of validation controls are present in the application?	Validation based on security, roles, and business logic exists at the field-level during data entry, post-data entry, and in bulk as a background process.
4.1.4		What are the options for application/security/process exception notification and procedures?	Exceptions are displayed to the current user and logged in the system for review by application administrators. For certain exceptions, administrators can also be notified via email.
4.1.5		Are the following controls maintained within the application: - Data Accuracy - Data Completeness - Data Integrity - Processing Exceptions	Data Accuracy - There are numerous edits plus multiple users review the work, further ensuring accuracy. Data Completeness – Validation rules prevent signoffs until all required fields are complete. Data Integrity – A comprehensive audit trail exists for all work and changes made in the system. Detecting Processing Exceptions – Exceptions, such as sending back work, are tracked and logged.

Ref.	Sub-Category	Question	Response
4.1.6		Do you use any open source? Please describe how patches are handled for the open source solution.	We use open source software on a limited basis (e.g., for non-security-critical features, such as rich text editing, charting, and UI widgets, as well as for our build and deployment systems). Due to the nature of these components, patching is very rare, and would be necessary only if we were to discover a bug.
4.1.7		Please describe your change management program utilized for all production changes in your environment.	We use a code migration process, facilitated by a version control system. Changes promoted to the production code thread require additional independent verification. Releases of production builds are driven via an automated deployment tool.
4.2.1	**Identity and Access Management**	Describe the method of authentication to gain access to the application.	SAML, ADSI, or built-in authentication.
4.2.2		Can the application be integrated with our Active Directory solution?	Yes, via either SAML or ADSI.
4.2.3		Please provide information on the user id and password controls within the solution. Detail the minimum password length, password expiration period, and minimum password age.	We use four levels of complexity, with administrator-controlled variables. The administrator can control the password variables, depending on each organization's policies.
4.2.4		Please describe the Federation protocols supported. How do we federate our existing identity store with yours?	SAML 2.0 is supported.
4.2.5		Do you allow your employees to bring their own devices and can the customers' information be accessed with these devices?	The application is delivered via a SaaS model on the public Internet. Therefore, it is accessible to all devices with Internet access, but only with proper login credentials.

Ref.	Sub-Category	Question	Response
4.3.1	**Batch Processing**	Is there a batch import or export process? Please describe when this process would be used.	There is a batch import process, designed for bulk user creation and bulk upload of reference data, as needed, from Excel. Workitems can also be batch exported via a ZIP file.
4.4.1	**Web Applications**	Please describe the security method used in the authentication and transmission of data.	Includes SAML, ADSI, built-in authentication, and SSL and database encryption, as noted in previous sections.
4.4.2		Please describe your approach to conducting pen testing on your environment and the frequency of running the scans.	Beyond the various automated tools described elsewhere in this questionnaire, we have also had detailed penetration testing conducted on behalf of (and paid for by) clients. To date, no significant vulnerabilities have been identified.
4.4.3		Do you share the results of your pen testing with your clients?	Yes, we are open to sharing pen test results.
4.4.4		What is your frequency for running audits against the application such as the OWASP top 10 Application Security Risk?	IBM AppScan is used to scan the software before every release.
4.4.5		Describe the encryption enabled between clients, databases and application servers?	Communication between the clients and the application servers, as well as from the applications server to the SQL database servers, are encrypted using SSL.
4.4.6		Is all data encrypted in transit to and from the service provider? If only a subset is encrypted, describe the details of the delineation.	Yes.

Ref.	Sub-Category	Question	Response
4.4.7		Please provide some information on whether your encryption within the application is FIPS compliant.	Since 2014, Microsoft specifically recommends disabling FIPS unless you are required to use it due to government regulations – which our clients have not been to this point.
4.4.8		Please describe your approach to vulnerability scanning (including authenticated and unauthenticated scans) and the frequency of running the scans.	Daily vulnerability scans are performed using Qualys, and IBM AppScan is used from an application perspective to perform dynamic scans per release. From an infrastructure perspective, the IDS performs daily vulnerability scanning.
4.5.1	**Server Patching**	Do third-party patches such as from Microsoft, Java, and Adobe need to be approved by your company before it can be applied to the respective servers?	Patches are applied based on Rackspace's deployment procedures.
4.5.2		Are there maintenance windows of downtime for routine server administration? When are they? Will the service always be unavailable during these windows or just some times? Will I get notifications when the service will be down during a maintenance window? How much advance notice?	Maintenance windows are typically monthly on the weekend for short periods, in the middle of the night. The application is always unavailable during those windows and notification is provided one week in advance.

5.0 Infrastructure

Ref.	Sub-Category	Question	Response
5.1.1	**Physical Security**	Please describe the physical access controls in place, including your data centers.	There are numerous controls, including but not limited to (a) security guards, (b) locks controlled by key-card/badge systems and/or biometric authentication, (c) closed-circuit video surveillance, and (d) termination and role-change control procedures.
5.1.2		Please describe the environmental controls in place, such as Fire Protection, Water Detection, Uninterrupted Power Supplies, Climate Controls, etc.	Standard, robust environmental controls are implemented in all Rackspace datacenters.
5.1.3		Are the environmental controls tested at least on an annual basis?	Yes - performed by Rackspace.
5.1.4		Is your data center monitored by CCTV cameras, with adequate retention of CCTV footage?	Yes - performed by Rackspace.
5.2.1	**Security Control**	Are you using virus protection software on all your computers (desktops, servers, and gateways)? Are all antivirus mechanisms current and actively running and capable of detecting, removing and protecting against other forms of malicious software such as spyware?	Yes.
5.2.2		Does your company utilize a solution to detect and respond to advanced malware, such as FireEye and Bit9?	Yes. We use Sophos Endpoint Security and Control for detecting and removing widespread and prevalent malware, including 0-day malware attacks, viruses, spyware, rootkits, Trojans, adware, and other potentially unwanted applications (PUAs).

Ref.	Sub-Category	Question	Response
5.2.3		Please describe your patch management program in place to deploy patches to your environment.	Patches are applied based on Rackspace's deployment procedures.
5.2.4		Have you deployed Firewalls and Intrusion Detection and Prevention Systems in your environment?	Yes.
5.2.5		Do you subscribe to the principle of “least privilege” and “need to know” access and authorization user management?	Yes.
5.2.6		Do you maintain a password security standard for all of the applications and systems in your environment?	Yes.
5.2.7		Are all users of your system uniquely identifiable (e.g., no shared accounts)?	Yes.
5.2.8		Can data be accessed by remote users accessing your production resources?	Yes. Remote access to Rackspace infrastructure is restricted to our support staff.
5.2.9		Is Multi-Factor Authentication implemented for remote access to your network by employees’ administrators and third parties?	Yes. Multi-Factor Authentication is required for remote access over VPN to our dedicated server environment at Rackspace.
5.2.10		Do you have formal, documented auditing and monitoring procedures for user accounts (creation, maintenance, review, protection, and retention)?	Yes.
5.2.11		Do you perform user access reviews for your employees, contractors? If so, what is the frequency of the reviews?	Yes.
5.2.12		Please describe the program and specific controls you have in place to manage and maintain unstructured data.	No unstructured data exists within the system.

Ref.	Sub-Category	Question	Response
5.3.1	**Logging and Monitoring**	Please detail your login and monitoring program.	Application Login information is logged. It is the client's responsibility to review these logs.
5.3.2		Do you implement system event logging on your server, database, and application environment that records at a minimum who, what, and when for all transactions?	Yes.
5.3.3		Do you review and analyze after-hours system accesses, as well as review logs for failed logins or unauthorized access?	Yes, see above.
5.3.4		Do you currently have a centralized log management solution such as SIEM in place and do you have a retention policy for logs?	Yes, see above.
5.3.5		Please describe the retention period for the various logs available within your solution	Log retention within the application is configurable to meet various security, business, and audit requirements.
5.4.1	**Wireless Security**	Do you currently have a wireless network in your environment? How is your wireless network secured?	Yes. Secured via WPA2. Firewall is in place. No guest access.
5.4.2		Do you conduct vulnerability testing and rogue access point scanning within your wireless network?	No. However, wireless networking is only available in our corporate environment. It is not permitted at the Rackspace datacenters.
5.4.3		Can customers' resources be accessed via the wireless network?	The application is accessible via any Internet-connected device.
5.4.4		Describe the authentication method used for wireless access.	WPA2 pre-shared key.
5.5.1	**Vulnerability Management**	Will customers be permitted to conduct additional assurance (e.g., annual desktop review)?	Yes.
5.5.2		Do you perform periodic vulnerability scans on your infrastructure?	Yes.

Ref.	Sub-Category	Question	Response
5.5.3		Do you have controls to prevent against Distributed Denial of Service Attacks?	We currently do not implement a technology solution, but are investigating a Rackspace service offering - Incapsula's cloud-based Web Application Firewall (WAF).
5.5.4		Do you contract with an independent third party to conduct a vulnerability assessment and/or penetration test on at least an annual basis and are findings remediated timely?	Third party assessments have been performed, but not on an annual basis. Any issues are remediated on a timely basis, based upon priorities agreed with the client arranging the test or assessment.
5.5.5		Are internal vulnerability scans conducted on at least a quarterly period?	Yes.
5.6.1	**Operations**	How many customers are using SAAS vs on-premises?	All customers are using SAAS.
5.6.2		Do you have capacity, license planning, and usage management?	Capacity and usage management is performed via tools provided by Rackspace and built into the application. Licenses are managed by Rackspace.
5.6.3		Do you have a program in place to monitor the colocation facility service provider?	We have been using Rackspace's full service offerings in a managed host environment, not a simple colocation service, for many years. We meet with them periodically to review the status of our implementations and their new offerings in which we may be interested.
5.6.4		Do you provide preproduction, testing and staging environments?	Yes.
5.6.5		Do you have monitoring and operational management?	Yes - performed by Rackspace.

Ref.	Sub-Category	Question	Response
5.7.1	**Network Design**	Please describe what firewall ports need to be enabled for the application.	N/A. The application is hosted at Rackspace.
5.7.2		Please describe the type of servers (either physical or virtual) required for this project.	N/A. The application is hosted at Rackspace.
5.8.1	**Disaster Recovery**	Do you have a comprehensive disaster recovery plan?	Yes - See accompanying Disaster Recovery Plan.
5.8.2		Do you test your disaster recovery plan on a regular basis?	Yes.