

SaaS IT Requirements Questionnaire

REQUIREMENTS

1. The provider is SOC compliant and can provide proof of it, if applicable
2. The provider is PCI compliant, if applicable
3. The provider is HIPPA compliant, if applicable
4. The provider provides LDAP and/or SSO integration
5. The provider has a disaster recovery option in place
6. The provider has a way to import and export data in a standard format
7. The provider has an API
8. The provider has the ability to generate reports against the data via direct data access or through their own report builder
9. The provider offers weekend and evening support (prefer 24x7)

QUESTIONS

1. Hosting Provider & Data Location

- a) Who is the hosting provider?
- b) Where is the hosting location? Country, State?
- c) Where is the primary data being stored?
- d) Where is the backup data being stored?

2. Data Access, Security, Segregation & Encryption

- a) Is it a dedicated or a shared environment?
- b) If it a shared environment, how is the data segregated from other shared environments?
- c) How is security managed in the shared environment? What controls are in place?
- d) How is the primary data being stored? Is the data in raw files or encrypted format?
- e) How is the backup data being stored? Is the data in raw files or encrypted format?
- f) What options are available to export the data, if at some point we wanted to move to another vendor? (i.e. CSV, SQL export, API, etc.)
- g) What options are available to import the data, if we want to migrate existing data from other systems into your current platform? (i.e. CSV, SQL, API, etc.)

3. Regulatory Compliance

- a) What types of regulations are being followed?
- b) PCI, HIPPA, SOC compliance? What options are available? How is this managed?
- c) How often are these being audited?
- d) How are these enforced?

4. Hosting Facility Security & Compliance

- a) Is the hosting facility SAS 70 II (Statement of Auditing Standards) compliant?
- b) How often is this compliance audited?

5. Business Continuity & Disaster Recovery

- a) Where are the DR (disaster recovery) data centers locations located?
- b) What type of infrastructure exists to replicate and synchronize data between the primary and DR data centers? Is this available in real-time, daily?
- c) If the primary environment is down? How quickly can the DR environment be made active either in the primary or the DR data center?

6. Identity Management, Security & Single Sign-On

- a) Is Single Sign-On (SSO) provided? What types of SSO options are available? SAML, HTTP-Fed, Open Auth, etc?
- b) Can the SaaS app be integrated with an existing Identity Management system?
- c) Does it support LDAP integration?
- d) Does it support dual-factor authentication?
- e) What type of other user security, authentication and authorization options are available?
- f) What level of support do you provide to support any of these integrations?

7. Standards, Policies, Procedures & Frameworks

- a) What architecture and technology standards do you follow?
- b) What development methodology do you follow?
- c) How often do you release changes to your environment? How are those changes communicated?
- d) What type of professional services do you offer to implement and support the SaaS application?
- e) Do you offer any implementation services?

8. Integration, APIs & Reports

- a) What type of APIs and web-services are available to pull and push data?
- b) Are the APIs secured and encrypted?
- c) Is there any documentation they can provide which speaks to the API?
- d) Is there an option to access the data directly from the database?
- e) What type of reports can be generated or created?

9. Support & Maintenance

- a) What type of support is provided? Self-service, email, phone?
- b) What are the support times? 24x7, 5 days a week?
- c) What are the support response times? Critical, Urgent, High & Low issues/requests?
- d) Who provides the support desk and where are they located? How many employees is part of the support desk? Dedicated or shared with customers?
- e) Is there a premium support model?
- f) What type of monitoring and alerting does the vendor provide?
- g) What type of migration and integration support does the vendor provide?
- h) Is there a dedicated support manager and account rep?
- i) How do you support and manage integration with the customer's existing SaaS apps?
- j) How are upgrades, patches and other maintenance performed?
- k) What type of change management & risk management procedures do you follow? How often is this communicated to the customers?
- l) Does the customer have any control on applying patches, upgrades and changes to the SaaS app? (this is very important to know especially if the SaaS app is integrated with other SaaS apps).

10. Service Level Agreements (SLAs)

- a) What SLAs are available – reliability, availability, performance, issues, requests, etc? Penalties?
- b) What types of credits are available if SLAs are not met?
- c) Are the terms & conditions of the contract tied to the SLAs?
- d) Is there a regular meeting (monthly/quarterly) to review the SLAs, issues, requests? If so, who takes part in those meetings from your organization?

- e) How are the issues escalated if the SLAs are not complied? Who can we escalate to in the management team?

11. Vendor Management, Product Road-map & Viability

- a) How long has the company been in business?
- b) How many customers do they have?
- c) What are their financials?
- d) What is the organization structure? How many employees? Where are they located?
- e) How many employees are there in the product development & support team?
- f) What is their product road-map and strategy? If willing to share – please provide any documentation around the product roadmap (planned features).
- g) How do they accommodate customer requirements into their product strategy? Is there a customer advisory council?
- h) Do you provide a trial or proof of concept for your product including new features?

12. Pricing & Contract

- a) What is included and excluded in the pricing?
- b) Will you charge for new product features?
- c) What is the minimum contract period? Are there any discounts for long-term contract? Is there an option to exit during the contract and what are the terms & conditions, penalties?