



formerly
Virtual Office News

Technology Tools for Today™

The **Only** Practice Management/Technology Newsletter for Financial Advisors.

Reprint from November 2011

Selecting an SaaS Vendor: What You Need to Know

By Stuart DePina, CEO, Tamarac Inc.



There are many advantages to using SaaS applications in your business:

- Virtual office - Accessible from anywhere with an internet connection
- No local server installation
- Rapid scalability
- System maintenance (backup, updates, maintenance, etc) included in service
- Security improvements
- Reliability and disaster recovery

When choosing a SaaS provider it is important to make sure you are selecting the appropriate vendor for your SaaS operations. Since many vendors are promoting “cloud” solutions, a critical

distinction to first evaluate is if the vendor is providing a truly Web-based SaaS solution, or are they simply making a desktop application accessible via the Web? There are significant performance, service and accessibility benefits for SaaS applications. Conversely, applications that were written to operate on a desktop do not translate well to Web access.

The following list of questions will help you in your vendor selection.

Data Center / Infrastructure

Effectively managing your client data is vital to the success of your business. When selecting a vendor you should make sure they host your data in a secure, scalable and redundant data center with a team that can support your business.

Q. Is the application hosted in the vendor’s private cloud or is it utilizing shared processing resources amongst other vendors? If the



Volume IX, Issue 11, November 2011

(C) Copyright 2003-2011
Virtual Office News LLC

Come Together

Find
the pieces
you need to
advance your
practice.

Learn to connect, integrate and transcend
at **T3: The Conference.**

February 16-18, 2012 – Hilton Anatole in Dallas, Texas



Technology Tools for Today™
Annual Conference 2012

Brought to you by conference producers, Dave Drucker and Joel Bruckenstein, Media partner, *Financial Planning* magazine

and sponsored by:



Ameritrade
Institutional



Tamarac®
the freedom to grow your business®

For registration details,
Sponsors Application and more visit
www.TechnologyToolsforToday.com

 twitter.com/t3fan

 [Blogger t3conference.blogspot.com](http://t3conference.blogspot.com)

vendor is using a private cloud, they are in full control of the performance of their application and can provide a consistent experience with their application.

Q. Is the data center SAS 70 type II compliant and is the latest report available for review?

- SAS 70 Type II Compliance ensures the data center enforces controls specific to operational performance and security to safeguard customer data.
- SAS 70 Type II audits are completed by a independent auditors annually and reports should be accessible once a Non Disclosure Agreement is in place.
- Ensure data center is SAS 70 Type II Compliant (annual audits) and not SAS 70 Type I Compliant (single audit).
- Is the data center going to upgrade to the new SSAE 16 service standard? (Effectively replaces SAS 70 Type II compliance as of 2012)

Q. Does the data center use an n+1 configuration?
Fully redundant HVAC (Cooling System) and UPS (Uninterrupted Power Supply). The N+1 configuration confirms that the data center is designed to withstand power or HVAC failures.

Q. How is monitoring configured?
Monitoring shouldn't be configured to only ping a server. Additional metrics should be set up (CPU Utilization, RAM, SQL, App, Services, etc.).

Q. Is fully redundant enterprise class routing equipment used?
There shouldn't be any single point of failure network devices in the architecture.

Q. Do fiber carriers enter the data center at disparate points to guard against service failure? Multiple carriers and multiple fiber entry points are essential to avoid Internet outages. In the event one fiber line is impacted the remaining circuits are designed to handle the Internet load.

Q. Are enhanced fire suppression devices in place and designed to stop fires from spreading in the unlikely event of a fire? Fire Suppression devices should be configured to isolate and extinguish a fire quickly.

Q. Is the data center secured with keycard protocols, biometric scanning, 24x7 interior/exterior surveillance monitoring and 24x7 onsite staff security? A data center must have all of these components to achieve SAS 70 Type II Compliance (and eventually SSAE 16) and is essential to the security of customer data.

Q. Are data center employees based in the United States and have they gone through thorough background checks prior to hire date? Some companies are required to have only U.S.-based employees manage their data or application.

Q. Can unauthorized individuals gain access to the data center without an escort? Unauthorized individuals should never have access to the data center without an escort.

Q. Are network and security teams certified? Certification is generally preferred due to expertise/experience level gained.

Q. Who has permission to access servers?

Permissions should be based on principles of least privilege, meaning permissions are restricted to only those authorized to perform work on the server.

Q. Are redundant firewalls and switches in use? Is failover automatic or manual? Redundant Firewalls and Switches should be implemented to remove a single point of failure scenario. HA (High Availability) mode or automated failover is preferred to reduce the likelihood of unplanned downtime.

Q. Is an intrusion detection system implemented? Intrusion Detection adds a layer of protection to your data. It should enforce threat modeling (attacker reputation, exploit type, behavior, etc.). Compliance reporting capabilities (GLBA, HIPAA, PCI-CISP, SOX) are preferred.

Q. Are backups available both onsite and offsite and what is the retention schedule?

- There should be both onsite backups (quickly accessible for immediate restores) and offsite backups (disaster recovery).
- Ensure backups include both data base and system files.
- Ensure there are weekly full backups and daily differentials/incremental. Offsite storage should be a 2 week rotation or longer.

Q. Are backup restores tested and how often? Backup restores should be tested at least once every 90 days. Testing once every 30 days is preferred.

Q. Are standby servers available? Standby servers are essential. In the event of a critical hardware failure a redundant system is required to quickly recover.

Q. Is there a business continuity plan (BCP) in place?

- A BCP must include both disaster prevention (high availability) as well as disaster recover (geographic redundancy).
- Process documentation should be available for review (with signed NDA).

Q. Is there geographic redundancy in place in the event of a disaster? This is generally available for an additional fee to increase SLA.

Q. Is infrastructure designed to scale and what are the growth plans of the data center?

- Monitoring should be configured to alert at specific capacity levels.
- Infrastructure requirements (new business, customer growth, etc.) should be reviewed quarterly and capacity increased as required.

Q. What are the support hours of operation how do customers access support (email, phone, knowledgebase, etc.)? This should be accessible

via a support process doc or on the vendor website.

Application / Data

One of the key benefits of working with a SaaS provider is the continual and seamless upgrades they can provide your organization. SaaS providers should also protect your data through both application security policies and data encryption while still allowing full access to your data to integrate with other systems.

Q. Is the application secure via SSL? Any web based application should use SSL for data security.

Q. How is data encrypted? A minimum of 128-bit encryption should be used.

Q. How is user authentication set up?

- Application should support only a single login per user ID.
- Systems should track multiple logon attempts, limit access and report to customer.
- Permissions designed on least privilege principle ideal.
- Utilize a stored procedure user authentication process to allow access to system database..

Is the application 100% Web-based? Does application require a client to be installed on end user machine?

Based on your policies you may not want a client installed on employee workstations.

Q. How easy is it to integrate the solution to other applications? Solution should utilize standard web API's to extract and upload data.

Q. Is the application customizable?

- Application is able to be branded.
- Customizable dashboards.
- Customizable fields and views.

Q. How often do upgrades or system enhancements happen? Every 30 to 60 days is ideal.

Q. Who owns the customer data and is it easily exportable? Client should always own data and have ability to export or receive full backups from vendor.

Q. Is application designed as a multi-tenant architecture? Multi-tenant architecture is preferred to reduce costs, offer higher performance and increase program scalability.

* * * * *

Stuart DePina is Chief Executive Officer of Tamarac, Inc. (www.tamaracinc.com), which provides an integrated web-based suite of

portfolio management software and outsourced portfolio management services to over 2200 advisors. Prior to joining Tamarac, DePina served in leadership positions for Who's Calling, xSides Corporation and Ticketmaster. Earlier in his career, he was a partner at KPMG, where he served clients in the firms' financial services practice.

