ITAK

Information Technology Asset Knowledge

Volume 8 Issue 4 Spring Conference

Drivin' ITAM Worldwide

Contingency Planning for SaaS

Does Your Contingency Plan Cover SaaS Applications?

By: **Frank Bruno**

Software as a Service (SaaS) applications are being integrated into many of today's business operations, but it is still an evolving form of technology consumption. As a result, contingency options for SaaS applications may be missing from your current business continuity plans because of the assumption that the cloud provider has it covered. However, did you know that 79% of all SaaS providers do not offer failover guarantees? This article explores the risks you may face when relying on SaaS providers, and outlines a framework for contingency planning that takes the risk out of SaaS.

The "What-if" Risks of Cloud Computing

Today's environment is tough for buyers and IT asset managers. You need to keep up with the latest and greatest technologies, but at the same time, you need to be vigilant about the reliability of your suppliers; are they going to stick around and be there for you over the long-term?

SaaS and cloud-based business application services are here to stay. Gartner predicts they will grow from $13.4 billion in 2011 to $32.2 billion in 2016, a five-year CAGR of 19.1%. (1)

However, new technologies, and the companies that supply those technologies, can be risky. A study conducted by *Inc*. magazine and the National Business Incubator Association (NBIA) revealed that 80% of new businesses fail within the first five years.(2) And, Softletter's 2012 SaaS Report states that SaaS providers are 40% more likely to go out of business than their traditional, on-premise competitors. (3)

It's hard to proactively adopt new technologies when there is a good chance that your supplier may not be around long enough for you to realize the return on your investment. You need to consider the risks before you enter into such an arrangement, especially for cloud-based services. Another point to remember is that with SaaS subscriptions, you are accessing both your application *and* data via the cloud. Physically, you do not possess the provider's software or your data. Therefore, you need to make sure that if something goes wrong, you can still access the application – and your data.

Chief Information Officers (CIOs) care a lot about their company's data, and need to make sure that it's secure, accessible, and usable. Without data, they're dead in the water. The mission of your CIO will impact the rest of the organization, which is why it's important to think like a CIO and understand their concerns. A smart CIO will put an Enterprise Program Management Office (EPMO) in place to create standards, policy, and manage the process to safely onboard new technology and the application portfolio.

So what about the SaaS delivery model? What are some of the risks to keep in mind when considering new SaaS applications? And what are the right processes to safely onboard SaaS providers? When we think about the risks of doing business, supplier bankruptcy is often top of mind. But it costs money to file for bankruptcy, leading some companies to skip this step and instead just disappear into thin air. As a result, their services are shut off due to non-payment, leaving you in a most precarious situation. You must think ahead to issues such as sudden cessation of business or force majeure, which prevents a provider from fulfilling its obligations under the contract. Another risk is failure to deliver in accordance with Service Level Agreements (SLAs), and data security. You also need to consider an exit strategy. What if you need to

change suppliers, but cannot recover your data – or worse, you don't know where your data is?

This is why it makes sense to assess the risks as a first step, and then establish a contingency plan that allows you to execute independently of the provider (and potentially, their suppliers).

Adequately Assessing the Risks

Did you know that 48% of SaaS sales fall through due to concerns about data safety and application availability? According to Softletter's 2012 SaaS Report, nearly half of all SaaS deals are scrapped because of these concerns. (3) What can you do about it? The first step is to assess the risks of entrusting your precious data to the cloud, and then determine whether you can adequately address each risk with a workable contingency plan.

Knowing how to identify and measure risk is important when you are contemplating a contingency plan. In fact, this should be a pre-requisite to creating a repeatable process for safely subscribing to new technology. To establish criteria around risk assessments, create a checklist of standard considerations for each SaaS application and how it impacts your business.

Be specific about numbers related to people, time and money in order to create an objective process for determining the right contingency solution. For example:

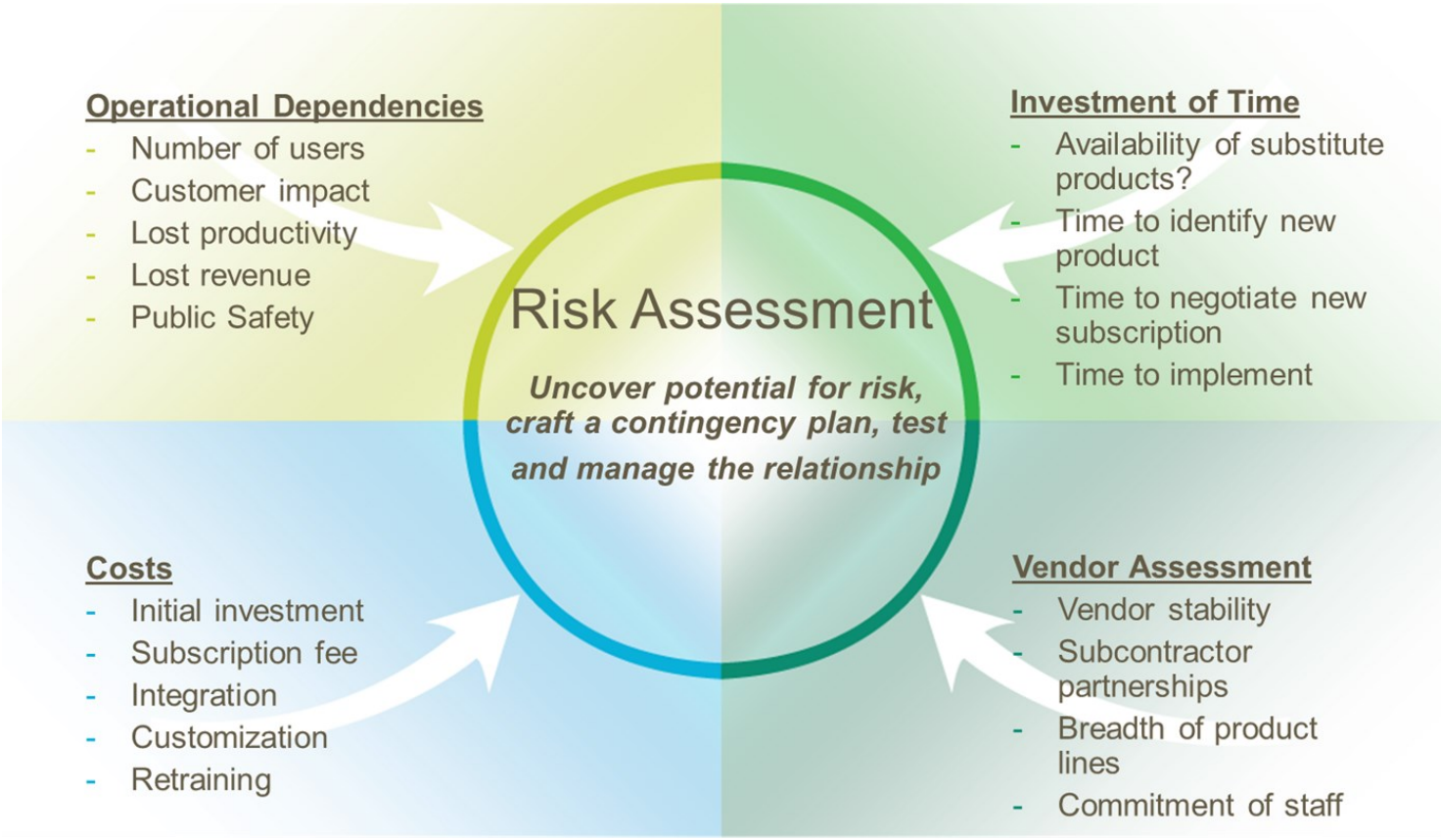
- **Operational Dependencies**: Is it a customer-facing technology? Does more than 20% of the organization use the technology on a regular basis? Does it impact productivity, revenue or public safety?
- **Costs**: Consider initial costs and potential replacement costs. Remember, the subscription fees are only a percentage of the total cost of ownership (TCO)
- **Investment of Time**: Will it take longer than one week to replace the service? Are there alternative services available?
- **Vendor Assessment**: How many years has the provider been in business? How many employees there know the technology? How many years has the service been in existence? Is it at the end of the "hype cycle"?

The math here is simple:

Operational Dependencies + Costs + Investment of Time + Vendor Assessment = Risk

Of course this general formula will not give you an exact calculation with a specific risk factor. For additional guidance, you can assign a risk score to each of your answers, based on a scale that represents the level of risk associated with the loss of the technology, for example, 1 means no risk and 4 means substantial risk. This will help give you an indication of the level of continuity service you will need for protection.

The resulting calculation will demonstrate the value of application to your organization and the value of protecting that technology. This type of calculation can help prove that contingency planning is critical to ensure application continuity.



More and more, we are also seeing companies who procure technology go through a checklist relative to Governance, Risk & Compliance (GRC). From the buyer's perspective, terms like governance, risk and compliance are fast becoming the juggernaut of the deal. Slowing deals down obviously doesn't help the business, so having a plan in place that addresses GRC makes for a win/win/win every time. It's a win for your company, who will effectively manage the risk and adequately protect its investments. It's a win for your supplier, who survives to live another day (figuratively speaking) and it is a win for you, who will successfully lead your company through the perils of the unknown.

Once the risks and GRC issues are identified, it's time to craft a contingency plan.

Contingency Planning for Application Continuity

You need access to your application and data no matter what happens to your SaaS provider's business – that's the main objective. The end goal is to flawlessly execute your contingency plan, thereby minimizing any lost time, productivity, revenue, and reputation. By anticipating problems – and preparing accordingly – contingency plans address the risk of extended outages and the other "what ifs" that you and your provider may face along the way.

Based on your risk assessment, here are some examples of contingency plans you may want to consider:

1. Take the application on-premises and maintain independently of the SaaS provider
2. Hire a Managed Service Provider (MSP) to host and maintain the application
3. Keep the lights on long enough to migrate data to a new solution

Depending on the variables involved, such as investment in the technology, the impact of an outage and the ability to support applications, any of these three contingency plans may be employed.

In some cases, it may be necessary to recreate the technology in-house, rather than source and implement new technology. However, in other situations, maintaining services long enough to migrate to a new solution is the best option. Regardless, it is absolutely critical that contingency plans are documented in advance of consummating the business relationship – and are verifiably capable of being executed independently of the SaaS provider.

At this point, you're probably thinking… this is a lot of work. Yes, contingency planning takes effort! That said, being cognizant of the fact that you need to plan for risk is a good start. Once you assess your risks and understand how they

impact your business, you will realize which contingency plan is optimal, and how you will overcome the risk objections to get the deal done.

As part of the contingency planning process, you should always communicate your concerns internally and externally. For the SaaS providers working to win your business, it makes good sense to anticipate your concerns and proactively address those risks by conceiving, crafting and testing the contingency plan. This demonstrates trust, and makes the buyer's job easier which lends to greater confidence in closing the deal.

One of the things that will address the risk is some kind of a document that stipulates where the data is and how it's being managed. That document may come through an SSAE 16 reporting on controls for a service organization (formerly SAS 70 Type II) or a systems information plan (SIP). The systems information plan needs to recognize where the data (every copy) resides physically. For example, if there's a primary server sitting in Pittsburgh, Pennsylvania with a back-up somewhere in South Philadelphia, then physical addresses are necessary as well as the Internet Protocol (IP) addresses. Additional details should include contact information for the people who touch those machines, information on how to access and run those servers, a clear understanding of the process by which they back up data at both facilities, and knowledge as to whether the old storage media has been destroyed (destruction certificates). The key is to have documented system information that you might need to access under certain conditions, if necessary. For the most part, it is a means to alleviate concern and to mitigate risk associated data security issues.

Now comes the true challenge; figuratively speaking, it's like trying to change a tire on a car that's traveling at 70 miles per hour. It is also the reason why 79% of SaaS providers don't offer a failover guarantee – because until now, there was no way to completely ensure against an extended outage or a sudden cessation of business. So, how do you execute the third contingency option outlined at the beginning of this section ("Keep the lights on long enough to migrate to a new solution")?

Let's consider the following formula:

Escrow Agent + Recovery-as-a-Service = Continuity Service Provider

For starters, it makes sense to entrust a neutral third party to maintain access to a recovery environment that is managed independently of the SaaS provider. A recovery environment can be a hot-site replicating in real-time with seamless failover – or something less sophisticated, depending on the desired Recovery Time/Point Objectives. The key is to have a mechanism in place that will allow the subscriber to execute their exit strategy without having to rely on the SaaS provider. Traditional source code escrow simply won't work here, but the escrow agents who know about the "what-ifs" of cloud computing can become "continuity service providers" (or "CSPs") and deliver the services you need to set your contingency in motion. Such "escrow-like" arrangements are the catalysts enabling your contingency plan to succeed – but they are not the plan in and of itself. The comprehensive benefits of contingency planning include:

- ✓ Application continuity
- ✓ Time to migrate to a new solution
- ✓ Unencumbered access to their data
- ✓ Timely access to components necessary to make use of data
- ✓ Leverage to optimize the vendor relationship (better response time and customer service)
- ✓ Satisfies governance, risk and compliance policy
- ✓ Minimize risk of loss
- ✓ Avoid litigation and the courts
- ✓ Allows focus on the vendor deliverables and benefits of SaaS

Of course, there is a lot more to it. Vetting the right Recovery-as-a-Service solution along with the best Continuity Service Provider (CSP) could be a challenge as well. Just as frustrating as it is to venture deep down the path with a SaaS provider to get to a "no-go" decision, you may find yourself doing the same thing with your CSP. If you don't feel as

though your prospective CSP is comfortable discussing contingency plans or how to help you accomplish the task, then you want to reconsider that decision too.

Triggering the Contingency Plan

So, how exactly does this all work? Let's say you're working with a SaaS provider that is prone to frequent outages, and you've discovered their service is rather poor. However, you didn't find that out until six months into the relationship – and now you want to get your data out so you can move to a new SaaS provider. You want to somehow migrate your data, and you want to do it safely - without any interference from your provider. It's not easy to execute an exit strategy without a contingency plan and the proper expertise. This is when working with an experienced CSP can help facilitate your management of the risks associated with SaaS providers, such as outages due to natural disasters, technical failures, sudden cessation of business, and bankruptcy issues.

Traditionally sought out as a measure of last resort, escrow arrangements provided software licensees with access to source code with the intent of replicating the licensor's application development environment and to independently maintain the software long-term. That was the contingency plan for licensees, triggered when the licensors went out of business.

With SaaS, the contemporary approach to "escrow" has now become a first line of defense, which can effectively save the day and probably someone's job. Standard continuity services provide the means to recover, and should be a pre-requisite to doing business, especially if there are designs to leverage SaaS in the enterprise markets and to entrust mission critical data to the cloud.

Triggering the contingency plan can be tied to any of the above referenced outages or some other condition involving non-compliance to service level agreements (SLAs) or the need for the business to simply change (i.e. termination for convenience). The bottom line here is that the contingency triggers should address all of the concerns that you have with a prospective SaaS provider as well as some that you may not have considered, hence the need for "convenience clause."

Effective Execution: The Devil is in the Details

There are so many clichés used to describe the same inference like "easier said than done" – and with SaaS application continuity, it could not be more evident. In order to ensure that the plan is going to work effectively, it is necessary to test the failover plan as often as you would conduct disaster recovery testing on mission critical on-premise applications. Auditing the system information plans complete with procedures that facilitate application access, basic support, functionality, data back-up and recovery is only part of it.

You also need to have a checklist of sorts to support the contingency plan as it relates to what your organization is going to do next (*i.e. Contingency Plan 1, 2 or 3 above*). That might include having pre-sourced a new solution and pre-negotiated contracts ready to execute if that is the exit strategy. Perhaps the technology is mission critical, in which case you may be making space in your data center to take the application on-premise. Verified source code may be sitting in a traditional escrow account with people possessing the requisite skill sets to support it.

Regardless of the path you choose, it makes sense that you have properly cased it out already, so you are ready – ready to recover, restore, and resume business operations. Here is the shortlist of topics that you must address each time you consider the cloud for technology:

- ✓ Contingency plan
- ✓ Contingency triggers
- ✓ Application continuity
- ✓ Neutral third party management
- ✓ Failover testing and frequency
- ✓ Data recovery
- ✓ Data migration and restoration
- ✓ Traditional software escrow and verification testing

These topical items are the key to an effective execution of your contingency plan. Otherwise, the outcome could be that your plan simply won't work. We can't stress the importance of over-communication when it comes to the risk assessment either. When it comes to securing buy-in from the business owners, it is critical that they understand the impact to the

business if something went wrong, not to mention the potential for personal pain that goes along with such disasters. The added cost may be unexpected, but it will also be comparatively far less than having to re-do everything. The best approach is to establish a repeatable process for dealing with such risk, and consistently executing every time to mitigate that risk.

Conclusion

In summary, contingency planning must align with the scope of disaster recovery. You need to plan for a wide range of triggers, including termination due to inconvenience for your business.

Obviously, this article was written from the perspective of protecting the subscriber's interest in SaaS, but for readers who represent the "sell side," there is something that you should consider as well. Having succession contingencies that allow your customers to leave at-will (or survive you in the event a sudden cessation of business) serves to establish the trust they need to forge a business relationship with you. It helps you to overcome sales objections pertaining to the perceived risk of your application, so that customers can focus on doing business with your company. Closing more deals faster will improve survivability in a highly volatile business environment, and even provide a competitive advantage in situations where, perhaps, other established SaaS providers that have not placed a priority on addressing said risks. In light of the growing adoption of SaaS, you need to figure out how to adequately protect your clients and mitigate risk associated with doing business with you.

Use this knowledge to avoid pitfalls. This includes adequately assessing the risk, planning for SaaS application continuity, and working with a trusted, neutral third party to ensure that you can execute the contingency plan effectively if needed.

References

- *Forbes, "Cloud Computing and Enterprise Software Forecast Update, 2012" by Louis Columbus, November 8, 2012, http://www.forbes.com/sites/louiscolumbus/2012/11/08/cloud-computing-and-enterprise-software-forecast-update-2012/*
- *Inc. magazine, "How to Avoid the Passion Trap" by Dave Smith, May 5, 2011, http://www.inc.com/articles/201105/how-to-avoid-the-passion-trap.html*
- *Softletter, 2012 SaaS Report, http://www.softletter.com/Research/SoftletterSaaSReport.aspx*