IRON MOUNTAIN®

CLOUD COMPUTING PROTECTION STRATEGIES

WHITE PAPER

STRATEGIES FOR SaaS CONTINGENCY PLANNING

CONTENTS

EXECUTIVE SUMMARY

The Software as a Service (SaaS) market continues to grow and gain significance as software delivery shifts from traditional onsite, licensed software to a cloud-based, on-demand SaaS model. Market analyst IDC forecasts that the worldwide SaaS market will grow to $53.6 billion by 2015 at a compound annual growth rate of 26.4%.[1] Gartner has a slightly more conservative forecast with revenue projections of $22.1 billion by 2015, from revenues of $12.3 billion in 2011.[2] In either case, SaaS cannot be ignored.

SaaS is the largest segment of cloud computing, leading the way for other cloud-based services, such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Growing almost five times faster than the software market as a whole, IDC predicts that the SaaS model will account for nearly $1 of every $6 spent on software by 2015.[3]

Small and medium businesses (SMBs) eagerly embraced SaaS, and were early adopters due to the benefits of its pay-as-you-go model and the ability to scale and upgrade. Experts believe that we are now at the tipping point for SaaS to move into enterprise organizations because many of the barriers to adoption, such as the IT department's concerns about the security of SaaS-based applications, are being addressed.[4] But, is that enough to fully mitigate the risks of entrusting mission-critical business applications and data to the cloud? Significant outages have been reported and some SaaS providers have announced cessation of business, without plans for helping their customers to recover their data and without transition plans. Lastly, if there is a dispute between the provider and the subscriber, how certain can you be that they will not (intentionally or unintentionally) imprison your data?

In this article, we will explore the strategic and tactical use of neutral third parties to enable SaaS contingency strategies as a way to mitigate some of the risks of SaaS and to keep users working. The article will also discuss how to establish contingency plans that can be used by SaaS subscribers to establish a repeatable process to ensure companies can safely and consistently invest in the cloud.

SaaS contingency planning can be used as a way to optimize the vendor relationship. For the SaaS subscriber, in addition to accessing source code, being able to maintain the software independently (bug fixes, enhancements, etc.) is the peace of mind that allows them to bypass the risk objections to doing business, so they can focus on doing business.

WHAT IS CONTINGENCY PLANNING FOR SaaS APPLICATIONS?

In any SaaS relationship, subscribers must consider the possibility that their provider may go out of business; undergo unexpected, significant outages; or experience other service interruptions. A SaaS contingency plan is intended to address these concerns and to enhance trust between the provider and subscribers.

Similar to traditional software escrow or technology escrow, critical software source code is stored with an independent, neutral, trusted third party. However, SaaS contingency plans protect, via escrow-like terms, your source code, object code, and data in a secure escrow account with a neutral third party. Some SaaS contingency services also provide continuous access to your data and standby failover services that enable Recovery-as-a-Service in order to achieve application continuity.

SaaS contingency planning can be used as a way to optimize the vendor relationship. For the SaaS subscriber, in addition to accessing source code, being able to maintain the software independently (bug fixes, enhancements, etc.) is the peace of mind that allows them to bypass the risk objections to doing business, so they can focus on doing business.

THE CRUX OF SaaS ENABLEMENT WITHIN THE ENTERPRISE MARKET

Questions about risk emerge as enterprises cautiously embrace cloud technology. There is no way to trust – beyond a shadow of a doubt – that the SaaS provider will remain a viable business long-term or that no catastrophic event beyond the provider's control will force a prolonged outage. Obvious concerns like bankruptcy and lack of support have always been release conditions in escrows, but with SaaS applications, these are now overshadowed by concerns relative to application continuity and the ability to access (or recover) mission-critical, proprietary data. Prospective SaaS subscribers are challenged with questions addressing concerns such as:

- What contingencies exist when a subscriber cannot access the SaaS application?
- What complexities occur with respect to replicating or maintaining the provider's live production environment? How hard is it to access data and is it usable without the application executable (structured versus unstructured data)?
- Would it be possible to sustain application continuity long enough to migrate to another solution?
- What is the contingency that extends beyond the provider's disaster recovery (DR) plan?
- Is it possible to execute the contingency plan independently from the provider?

HOW CAN YOU OVERCOME THE RISKS OF SaaS?

In light of this bourgeoning software delivery model, SaaS subscribers are still figuring out how to adequately protect their investments and mitigate risk associated with entrusting their mission-critical applications (and data) to the cloud. SaaS contingency planning helps to overcome these risks.

The need for escrow is, of course, based on the requirements set forth by the subscribers and it depends on the perceived risk. For example, if a SaaS application is used by a small number of users and the data is not mission critical, a company might be able to adequately address the risk by requesting periodic copies of the data for migration purposes – without the need for escrow.

On the other hand, a SaaS deployment to thousands of users, which entrusts the most mission critical data to the cloud, is a prime opportunity for SaaS contingency planning. In this example, it becomes the fiduciary responsibility of the company to have contingency plans with an escrow release as a trigger to set that plan in motion. In this way, escrow can be the "SaaS-enabler" to the enterprise markets.

There are also intrinsic benefits to SaaS providers for implementing a SaaS contingency planning arrangement. SaaS providers are finding that offering escrow is a proactive way for them to instill trust with their customers and to overcome business risk objections so that the parties involved can focus on doing business.

CONTINGENCY PLANNING AND EXECUTION

Another consideration before implementing a SaaS solution is a thorough understanding of viable contingency plans. What options exist if there are problems with a SaaS provider? Many times, SaaS subscribers think they are covered by their provider's disaster recovery plan, but this is a huge misconception.

Here are three basic contingencies for subscribers:

1. **Take the application onsite and maintain it independently of the SaaS provider.**
2. **Find a new Managed Service Provider (MSP) to support and/or host the application.**
3. **Keep the lights on long enough to source and migrate data to a new solution.**

Depending on the variables (investment in the technology, the impact of an outage and the ability to support applications), any of these contingency plans may be employed. With a SaaS contingency plan in place, SaaS subscribers will have the means to move forward. Whether just the source code is needed or a complete failover service is required, with a contingency plan, the SaaS subscriber can rest assured knowing their data is protected.

In some cases, it is cheaper to recreate the technology in-house than to source and implement new technology. In other cases, maintaining services long enough to migrate to a new solution may be the best option. Think of this as taking a bus on a trip. If the bus runs out of gas, you wish you had a spare gas container that could temporarily fuel the bus until you safely reach a point where you can refuel or switch buses, so you then can continue the journey. You don't want to build a new bus to continue your journey because it can be way too costly, time-consuming, and complex. In this analogy, the SaaS contingency plan with failover is the spare gas needed to safely reach that switching point.

Regardless, it is absolutely critical that contingency plans are documented in advance of consummating the business relationship. With a SaaS contingency plan in place, subscribers can make sure they are capable of executing the contingency plan independently of the SaaS provider.

THE BENEFITS OF CONTINGENCY PLANNING FOR SaaS

Let's consider the benefits of contingency plans for SaaS as they relate to instilling trust between the buyer and seller. By securing the trust, the parties can move past the contractual negotiations and focus on the relationship.

For the subscriber, the main benefits of implementing a SaaS contingency plan are to:

- **Protect** the investment in the provider's technology.
- **Comply** with the Governance, Risk and Compliance (GRC) policy.
- **Optimize** the vendor relationship (bypass the risk objection to doing business, so you can focus on doing business).
- **Enable** successors who would be responsible for maintaining the technology for the purpose of ensuring application continuity long enough to recover data and to migrate to a new solution if necessary.

No one wants to think about their SaaS provider failing, but vigilance is essential. It is important to know the warning signs that could eventually lead to an untimely demise of the provider. For instance, repeated calls for support are addressed with slower response times. The people that you know and trust begin leaving the provider's company. Social media blogs citing problems with the provider or any negative specific industry news should perk up your sensitivity. If you are ever faced with problems, a SaaS contingency plan that includes an escrow agreement gives you the ability to execute an exit strategy, application continuity to access your data, and to facilitate an orderly transition to another provider. The escrow agreement is the mechanism to trigger the contingency plan.

So we have introduced you to what is believed to be the crux of SaaS enablement. We have exposed the risks, the questions, the various contingencies, and the benefits of a contingency plan, and now we will explore the guidance necessary to execute a practical and purposeful escrow arrangement to secure trust in SaaS.

THE RIGHT GUIDANCE

The goal of SaaS contingency planning is to enable SaaS by instilling trust. Adequate escrow protection includes a documented tactical contingency plan to either maintain the technology independently or to allow for enough time to migrate to a new SaaS solution. With this in mind, the following steps should be followed to establish contingency plans and to protect the subscriber's interest in SaaS.

1 STEP ONE

Before considering SaaS as a solution to a business need, be clear on how the SaaS technology is delivered. If delivered via a third-party MSP, make sure your pre-qualification procedures are comprehensive before proceeding down the Request for Proposal (RFP) path. As a condition of doing business, insist on a contingency plan that extends beyond the SaaS provider and work with an experienced escrow agent who can provide the right guidance.

2 STEP TWO

Determine your contingency plan based on the size of the investment (time + money + effort + opportunity cost, etc.). Will there be a need to potentially take the application onsite or find a new solution provider? Is it necessary to include the MSP in the contingency? Determine what triggering events (release conditions) support the contingency plan. How will you document the contingency plan? Who will be responsible to execute the contingency plan? These are just a few of the questions that must be addressed before moving forward.

3 STEP THREE

Document your contingency plan with specificity. Do not execute any business agreements until your contingency plan is complete. If possible, test your contingency plan before executing any business agreements. If this is not possible, then make sure verification testing of the contingency plan is a contractual obligation of your business agreement (via an escrow agreement).

4 STEP FOUR

Conduct verification testing. Verification testing can be as simple as making sure the mirrored environment will work when needed. It could be as comprehensive as traditional source code compilation and functional testing. The good news is that for the majority of subscribers, simple access to the recovery environment is all that is necessary to ensure contingency and to "have enough time" to migrate data. It is also important to test how easily the data can be recovered for purposes of migration to a new solution.

5 STEP FIVE

Establish a well-documented, repeatable process for safely onboarding new technology and socialize this within your organization. Maintain a copy of it within your company's document repository and/or procurement/ contracting procedures manual.

CONCLUSION

In conclusion, consideration should be given to creating a deeper back stop by implementing a SaaS contingency plan as an integral part of your SaaS application deployment.

Our guidance can be summarized in these five steps:

1. **Due diligence: understand potential fail points and insist upon a contingency plan that can be executed independently of the provider.**
2. **Determine your contingency plan based on the size and value of the investment.**
3. **Establish a well-documented arrangement to facilitate the contingency plan.**
4. **Test everything to verify the plan works.**
5. **Adopt a repeatable process for consistently and safely onboarding new technology.**

The key to overcoming the risks of SaaS is demonstrating that you have planned for these concerns and have taken the appropriate action to adequately address them. A comprehensive SaaS contingency plan is, in essence, a powerful risk management tool for companies involved on both sides of SaaS relationships. By assuring application and data availability, SaaS contingency plans help to foster trust between all parties.

REFERENCES

Adapted from an article originally published in ITAK Volume 7, Issue 9.

Note: The original term "SaaS escrow" was updated to "SaaS contingency planning" in this white paper because it has a broader scope and reflects the current recommendations.

[1] IDC Worldwide Software as a Service 2011-2015 Forecast, August 2011, http://www.idc.com/research/viewtoc.jsp?containerId=229440

[2] Gartner Says Worldwide Software-as-a-Service Revenue to Reach $14.5 Billion in 2012, March 27, 2012, http://www.gartner.com/it/page.jsp?id=1963815

[3] IDC Worldwide Software as a Service 2011-2015 Forecast, August 2011, http://www.idc.com/research/viewtoc.jsp?containerId=229440

[4] SaaS for Enterprises Approaches Tipping Point, March 19, 2012, http://www.webtorials.com/discussions/2012/03/saas-for-enterprises-approaches-tipping-point.html

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks, and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.