



## How Software as a Service (SaaS) Providers Can Instill Customer Confidence

# Table of Contents

Introduction .....	3
How Do SaaS providers Instill Confidence? .....	3
First Let's Start with What Is a SaaS Escrow? .....	4
And What About the Data? .....	4
How Does This Benefit the SaaS Provider? .....	5
How Do SaaS Providers Put in Place an Escrow Arrangement that Covers All of This? .....	5
How Much Does This Cost and Who Typically Pays for This Kind of Escrow? .....	5
Final Thoughts .....	6

## INTRODUCTION

In the early days, Application Service Providers (ASPs) surfed up alongside their internet “dotcom” brethren to ride the wave of prosperity. As the internet became ubiquitous to the computing world, application services emerged as a next logical step in the evolution. Conceptually, the thought of not having to invest in infrastructure or head count to support an application was attractive to business owners. However, this value proposition would soon freeze in time like a prehistoric corpse settling in for the Ice Age.

You see, CIOs hated the idea because of the threat to their very existence. The thought of replacing servers, people and on premise software with outsourced subscription services put ASPs at an early disadvantage. Furthermore, compromising the economics, data center capacity, security, scalability, application latency and interoperability (and potentially a good portion of the IT budget addressing these issues), quickly put ASPs in the history books.

But, fast forward the clock to present day IT and most of these issues have been addressed. The concept is still sound and the value proposition is compelling enough to revive the market. Terms like “SaaS” (Software as a Service) and “on-demand” have been coined to distance the service from the past, and cleanse the market of its old reputation. As this market continues to gain traction and attract new venture capital, business owners, and even CIOs, are ready to take advantage of the benefits of SaaS. However, SaaS subscribers must still beware of the unforeseen.

What happens if a SaaS provider sustains an extended outage, or worse, disappears forever? The same concerns faced by traditional licensees of mission-critical software abound here in triplicate as subscribers search for safe ways to address the risks of entering into a SaaS relationship. After all, an occurrence such as this one not only affects the user’s ability to support the application, it prevents them from accessing the application and their data altogether!

## HOW DO SAAS PROVIDERS INSTILL CONFIDENCE?

As companies continue to consider SaaS solutions, the protection strategy that has been most commonly utilized has been the technology escrow.

Technology escrow is a commonly used arrangement that engenders trust between a licensor and licensee in a traditional on-premise software deal. The agreement calls for the software developer or licensor to put their intellectual property (source code and related materials) into the care of a neutral third party (the Escrow Agent) for the benefit of their licensees should there be a need to gain access to the deposit materials. This arrangement provides protection to software licensees in the event the software provider goes out of business or discontinues support of the application. The source code enables them to continue supporting the application independently from the licensor. Thus, the mere threat of this occurrence motivates licensors to live up to their obligations set forth under the licensing agreement.

As many software vendors continue to migrate to the SaaS delivery model, there are significant changes in the way users contract for the technology. The one thing that hasn’t changed is the way an escrow is employed to engender trust between the two delivery models. This is a problem. While a traditional escrow arrangement protects licensees by enabling them to recreate the application development environment of the software, they still have a live production environment (and their data) supporting the needs of their end users. SaaS does not require the subscriber to maintain a live production environment or their data, which means that an outage could be a huge problem.

In an escrow agreement set up specifically to address the needs of SaaS, source code alone will not satisfy the needs of these end users because of the time it takes to recompile the executable, not to mention, the time it takes to gain access to their data. Consider the Recovery Time Objective (RTO) and the Recovery Point

Objective (RPO), two terms commonly used in disaster recovery and business continuance plans to describe how long it would take to get back on line and the point in time to which the data must be restored. You see, a typical escrow release process takes time; sometimes up to 60 business days. Then there are the challenges associated with utilizing the source code to recreate an application development environment and subsequently re-loading the application and data into a run-time environment. Unless the business can sustain that kind of an outage, it is strongly recommended that companies ask for access to object code and their data.

Most SaaS providers have yet to come to grips with this reality; viewing the executables (the deliverables of Software as a Service) as their intellectual property, without which they cannot derive recurring subscription fees. The good news is that the SaaS provider can gain a lot of confidence from their prospects and clients by entering into what we'll refer to as a "SaaS escrow." We'll cover the benefits of a SaaS escrow later in this article, but suffice it to say that the SaaS escrow will enable the subscriber to recover from an extended outage according to their desired RTO and RPO.

### **FIRST LET'S START WITH WHAT IS A SAAS ESCROW?**

Essentially, the SaaS escrow is an agreement involving the SaaS provider, the Subscriber and the Escrow Agent. It involves two separate deposit accounts that are managed by the terms and conditions of the Escrow Agreement. The first deposit account contains the source code, which is governed by traditional release conditions (bankruptcy, failure to support, etc.) also referred to as "notice release." The second deposit account should contain the object code and data, which would be governed by a more urgent set of release conditions, which we refer to as "demand release." For instance, if a subscriber sustained an outage that lasted for 24 hours or more, they would invoke their right to demand release of the object code and data.

Of course there is more to it than just object code and data. There are the build instructions to recreating the run-time environment, description of the hardware stack, other application protocol interfaces, instructions on accessing and integrating data, back up hosting solutions, etc. These are all line items that need to be checked off and verified as they are completed, prior to commencing the SaaS relationship.

Like any other mission-critical software application, companies perform disaster recovery testing to ensure business continuity. Especially if business regulations such as the Sarbanes-Oxley Act (SOX) or the Health Insurance Portability and Accountability Act (HIPAA) impact the application, companies can suffer stiff penalties for non-compliance. The risk associated with leaving it to the SaaS provider alone can be consequential. Therefore, it makes sense to have this testing performed and verified by a neutral third party who can attest that industry-standard steps were taken to verify the recovery time objectives of these SaaS applications. Only then, can you be truly sure that the subscribers will gain usable and productive access to the application and their data.

### **AND WHAT ABOUT THE DATA?**

Securing access to the data can be tricky depending on the current back-up systems in place to ensure full recovery and data freshness. If the SaaS provider is backing up to physical media and storing off site, certainly data freshness might be an issue, but subscribers will likely note this as a competitive differentiator during the vendor selections process, especially if the recovery point objectives are less than one day.

If a SaaS provider contracting with a back-up hosting partner to mirror data, then the data freshness should not be an issue. However, there is always the fear of this critical relationship souring. After all, when a company begins to fail financially, they tend to fall behind on payments and this could result in service interruptions. Subscribers should look for provisions to gain notice of this type of occurrence. They may also look to assume the rights and responsibilities of the SaaS provider (under that agreement) in the event of a

default, and in an attempt to recover their data and to sustain the application if the executable is available through the back up hosting company. In this scenario, the SaaS escrow (demand release) deposit would simply contain these assignments that would provide the subscriber with the authority to cure the default and to access their data.

Escrow Agents specializing in SaaS escrow should also be able to offer data back up services, which would also serve as the deposit materials contained in the second (demand release) deposit account. Subscribers would likely prefer this method as the escrow agent can act as the coordinator of this set up and verify that everything will work as planned in the event of an outage.

### **SO HOW DOES THIS BENEFIT THE SAAS PROVIDER?**

Well first, the SaaS provider can gain competitive advantage over other companies by proactively addressing the escrow requirement of the subscriber. Subscribers have become savvier over the years and many of them require escrow security as a policy for safely on-boarding new technology. Providing SaaS escrow may also help to shorten their sales cycle by lessening the number of objections to overcome. Additionally, there could be significant marketing value associated with having the escrow in place. Many companies advertise the practice of using escrow on their websites as a way to emphasize their commitment to client security.

### **HOW DO SAAS PROVIDERS PUT IN PLACE AN ESCROW ARRANGEMENT THAT COVERS ALL OF THIS?**

First, find an escrow agent that you can trust. Many escrow agents will advertise full services on their website, but the bricks and mortar behind the façade may not support the truth. Additionally, the expertise providing the guidance must instill brand confidence. Always look for an agent that maintains a solid reputation in the industry and if necessary, go see the facilities for yourself. After all, it is your intellectual property.

Second, use an agreement that is designed to accommodate SaaS escrow services. Again, you want to have dual deposit accounts with separate sets of release conditions governing each appropriately. Linking clients as beneficiaries to the deposit accounts is as simple as executing an enrollment form, which also obligates them under the terms and conditions of the agreement.

Concurrently, work on the deposit materials. The first deposit account should contain all of the components necessary to recreate the application development environment. The second deposit account should contain all of the components necessary to recreate the live production environment. Work with the escrow agent to develop a Statement of Work to verify both the source code deposit as well as the object code and data deposit. The most important aspect to the exercise will be to validate the instructions to affect a positive outcome. Like a fire drill for safety, being able to recreate the live production environment according to the desired RTO and RPO will ensure that no one gets burned.

### **HOW MUCH DOES THIS COST AND WHO TYPICALLY PAYS FOR THIS KIND OF ESCROW?**

Determining the actual cost of setting up a SaaS escrow depends on what the SaaS provider is willing to do to attract new subscribers. To simply put a traditional escrow agreement in place will cost approximately \$4,000 - \$5,000 excluding renewal fees and verification testing. Fees for Verification testing will vary depending on the complexity of the software and the environment that it runs on, but a fixed price Statement of Work can be obtained for budgeting purposes. It is highly recommended that disaster recovery testing take place to ensure a successful recreation of the live production environment. Again the costs associated with this exercise will vary, but can be obtained in advance with a completed pre-testing questionnaire. Lastly, let's not forget the data, which depends on the capacities stored and the recovery point objectives. Generally, data in the 50-100 GB range backed up once every hour, will run \$7,500 per year, but overages can add significant expense to this estimate.

In any contractual arrangement, the cost is typically negotiated as a condition of doing business. Taking a proactive approach to escrow allows the SaaS provider to institute policies that shift the burden of cost over to the subscriber. Many SaaS providers can also offer this as a value added service charged at a premium to what the SaaS provider paid to put the arrangement in place. Of course, if you average the cost across your entire client base, SaaS escrow can be justified as an investment to attract new business.

### FINAL THOUGHTS

SaaS is trending upwards. Business owners who want to reduce cost and focus on the core competencies that drive their business are supporting it. Venture capital is showing up in force and CIOs no longer seem too concerned about issues that plagued ASPs during the early days. Unfortunately, no one possesses the crystal ball that will allow the subscriber to see into the future. It only takes one instance of a disaster in the news to cause a shift in demand. Therefore, the only way to ensure that demand for SaaS will remain healthy is to have a SaaS escrow in place as a contingency plan that responsibly addresses disaster recovery and business continuity concerns.

### ABOUT THE AUTHOR

FRANK BRUNO is a manager for Iron Mountain Intellectual Property Management services, and consults with developers, corporations, and intellectual property law professionals throughout the United States on IP management best practices. He has spoken at many professional and industry events, including the NCMA World Congress, IACCM Annual Conference, IAITAM Annual Conference, and Caucus.

**Disclaimer:** This white paper may be redistributed in its entirety provided that the copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. These documents are provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Iron Mountain. The listing of an organization does not imply any sort of endorsement and Iron Mountain does not take any responsibility for the products or tools listed.

© 2007 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



**IRON MOUNTAIN®**  
745 Atlantic Avenue  
Boston, Massachusetts 02111  
(800) 899-IRON

Iron Mountain Digital, the world's leading provider of data backup/recovery and archiving software as a service (SaaS), offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world. For more information, visit our Web site at [www.ironmountain.com/digital](http://www.ironmountain.com/digital).