White Paper: Mitigating the additional risks of software-as-a-service applications.

A resource for technology decision makers to identify and mitigate the additional risk factors of SaaS applications.

PRAXIS Technology Escrow, LLC
Chris Smith
Founder & CEO

White Paper: Mitigating the additional risks of software-as-a-service applications.

Software-as-a-service, or SaaS, has become the new preferred method of utilizing technology for many corporations, healthcare organizations, universities and government entities. The benefits of cloud computing can dramatically reduce costs, speed-up implementation and training, and provide tremendous capabilities for remote users. Because SaaS applications are often significantly less expensive initially than on premise applications, the due diligence performed by end-user organizations prior to implementing SaaS applications is often less thorough. As a result, many end-users are unaware of the additional risks present in software-as-a-service applications.

Traditional Risks of On-Premise Software

Software, whether it is deployed on premise or in the cloud, has always presented a certain level of risk in the event of vendor failure. Vendor failure is often thought to consist only of bankruptcy but there are many other types of failures (i.e. breach of support, price increases, “sun setting” & more) that affect technology companies and subsequently their end-users. In addition to the traditional risks of the software company potentially going out of business at some point and leaving the end-user without proper support, software-as-a-service applications represent additional risk factors above and beyond those present with an on-premise application.

Additional Risk Factors of SaaS Applications

Immediate / Permanent Downtime - While a stable on premise application may run for years after a software company drops support for the product, the same typically cannot be said for SaaS applications. With a hosted application, downtime can result in immediate loss of functionality for the end-user. During downtime, in most cases, the end-user will not have access to their data. Thus, business critical functions provided by SaaS applications can cease at any moment

depending upon the viability of the software provider, hosting provider and even internet service.

Data Loss - Many of today's SaaS solutions contain the end-user's data within the solution and often is not readily available to the end-user. Many SaaS companies do this to make their client more dependent upon their services. In other words, this makes it difficult for the end-user to change software providers. However, if the software company goes out of business and stops paying their hosting provider, the hosting provider is most likely to delete the application and data in a short period of time. In most cases, the hosting company does not know who the end-users are. Therefore, no warning is provided for the end-user. So in the case of the data being held within the application itself, data loss can be immediate and permanent.

Data Migration - In the event of a software company failing to support a SaaS application or going out of business, the end-user can always migrate to another solution, provided that the end-user has access to a recent and functional back up of their data. However, simply having a functional copy of data does not mean that a migration will be fast or inexpensive. Data migrations can be costly and in some cases, take weeks or even months to complete. This is another factor that should be addressed when considering a SaaS application.

Open Source - Another risk factor in any software escrow situation is the possibility that the software contains open source tools and the escrow agreement might violate the General Public License (GPL). It is possible that placing open source code into escrow would violate the GPL and could potentially lead to significant damages for the software company and potentially the end-user. For this reason, it is important to fully understand the licensing implications of any open source code that your depositor would place into escrow. Alternatively, the software vendor may simply include a list of any required third-party tools, open-source or not, in the escrow deposit materials so that the end-user can obtain and license the requisite technologies to run the software.

Agile Development - SaaS applications are often built using agile development methods that mean the source code may be changing daily or weekly as opposed

to the traditional releases of versions that are common in waterfall development. Most traditional escrow agreements only require that the software company update their escrow deposit materials 2-4 times each year. In an agile development environment, this virtually guarantees that the escrow deposit will be outdated and thus of less value to the end-user in a release scenario. There are several additional risk factors in a SaaS environment that can be addressed but are often overlooked by end-user organizations. In many cases the solutions to these additional risk factors are relatively easy and inexpensive to implement.

Solutions to Address SaaS Related Risks

Continual Escrow - PRAXIS provides a method for software developers to connect their source code version control archives (i.e. GitHub, Bitbucket & etc.) directly to their digital deposit account so that the source code is updated on a continual, near real time basis. PRAXIS also performs scheduled backups of the complete environment creating an archive of historical versions for long term purposes.

Data - There are multiple ways to ensure that the end-user has access to their data. In many cases, the SaaS company will provide the data directly to the end-user on a scheduled basis. Additionally, the end-user may be able to require an online backup solution and many escrow agents, including PRAXIS, will provide escrow protection for their data through their escrow solution.

Multi-Tenant Environments – Some SaaS applications are built in true multi - tenant environments where all users access a single instance of the application running in the cloud and their data may be stored in one database but controlled through the permissions enabled in the database. While this shared environment dramatically reduces computing power and storage requirements it may also mean that data for any given end-user cannot be easily extracted. Thus, in some enterprise SaaS applications, end-users insist on private cloud versions of the application.

Application - Application continuity is an important component of any business continuance plan whether the technology is on premise or in the cloud. In some cases, the application would need to be regenerated by the end-user upon

release from the escrow. The end-user would certainly need access to updated source code, documentation, build instructions and other information that would help them to recreate the application with the help of a reasonably skilled software engineer. In more mission critical scenarios, it may be worth considering establishing a redundant, "ready state" environment to serve as a "hot site".

Know How - An increasingly popular method for protecting software applications is to capture as much "know how" as possible in the escrow agreement and the associated escrow deposit materials.

Examples of "know how" that can be included in the escrow are as follows:

- Contact information for key personnel that support the software or software-as-a-service application.
- Disclosure and full credential information for the hosting solution in a SaaS environment.
- Language that voids any non-solicitation clauses in the software license or software subscription agreement to provide the end-user with the legal permission to hire the key personnel to support the application.
- Full disclosure of the hosting provider, login credentials, etc. so that the end-user can simply continue to utilize the application in its current environment.

Transition Services - Many new SaaS escrow agreements today include what can be defined loosely as transition services to enable the end-user to easily and efficiently continue to support the application where it is currently hosted or migrate to another provider should a release condition occur. In some cases, transition services are negotiated in detail including billing rates, durations, etc. PRAXIS can provide sample clauses to be included in your escrow agreement.

Summary

SaaS applications have been widely adopted because of the many benefits that they provide but most organizations have not yet put measures in place to adequately protect themselves against the additional risks that are present in SaaS solutions. Advances in replication and data backup technology as well as the dramatic reduction in costs of storage and computing have made the solutions to many of the additional risk factors easy to address. Further, best practices related to capturing and transferring critical "know how" and the embedding of transition services into the escrow agreement have made mitigating risks of SaaS both easier and less expensive to implement.

About the Author

Chris Smith is Founder and CEO of PRAXIS Technology Escrow, LLC and a veteran of the technology escrow industry since the late 1990's. Throughout much of the past three decades, Chris has helped financial institutions, Fortune 500 companies and countless software and technology companies implement customized technology escrow solutions. Chris has held executive level positions with Iron Mountain, the NCC Group and was Co-Founder and President of Escrow Associates, LLC which was acquired by NCC Group in 2011. Throughout his career Chris has been an educator and is certified to deliver continuing legal education (CLE) courses in several states.

About PRAXIS Technology Escrow, LLC

This white paper was written for technology leaders and decision makers of corporations, healthcare organizations and governmental organizations who are considering risks related to SaaS applications. PRAXIS is a worldwide provider of highly customized software and technology escrow services based in Atlanta, Georgia.

PRAXIS Technology Escrow, LLC (800) 213 9802 / (770) 459 1202
www.praxisescrow.com or info@praxisescrow.com