Prepared for:

NRF | tech 2018

RETAIL'S PREMIER TECHNOLOGY SUMMIT

THE ULITMATE GUIDE TO SAAS CLOUD SUBSCRIPTION AGREEMENTS

Often complex and vendor-centric, cloud subscription agreements require a unique negotiation approach even though they can sometimes resemble more traditional on-premise contracts. Enterprises turning their attention to and adopting SaaS applications must approach their cloud agreements with the proper rigor and ensure they include necessary upfront and downstream protections as well as flexibility while also addressing various security concerns. Though cloud vendors will often insist that they are unable to modify their standardized contracts, it is possible to negotiate adjustments with the right approach. This white paper reveals actionable strategies for ensuring your cloud agreements provide long-term value and protections.

UpperEdge

Table of Contents

Section 1

Key Considerations and Caveats for SaaS Cloud Contracting

There is no doubt that the emergence of cloud, and specifically Software as a Service (SaaS), has been one of the most profound technology developments in the last decade. Enterprises in a wide range of industries are turning their attention to—and adopting—SaaS solutions at a rapidly growing rate.

SaaS solutions offered by cloud vendors such as Salesforce, ServiceNow, Workday, as well as larger IT vendors like Microsoft, Oracle and SAP, have become popular within enterprises over the last few years largely because of the promised ability to:

- Cut costs
- Reduce implementation timelines
- Provide flexibility not typically found in more traditional on-premise software arrangements.

However, the reality of SaaS has not exactly fulfilled the promise. And to a considerable extent, that's due to contracting issues and challenges.

As more enterprises adopt or at least begin to evaluate SaaS models, it is imperative that they separate hype and potential from facts and best practices. Specifically, they should treat their **SaaS cloud subscription agreements** with the same level of attention and due diligence as they do more traditional software licensing arrangements.

Are You Fully Reaping the Value of SaaS?

A few common misconceptions and contracting missteps often hinder the full realization of the **SaaS value proposition**. For instance, most SaaS cloud subscription agreements don't reflect a truly on-demand highly flexible model and are not structured for precision metering of actual consumption. Rather, they look more like traditional, on-premise software contracts, with fixed fee payments for a specified set of products and a committed number of users.

What's worse, the expected commitments are set in stone for multiple years, with obligations to make upfront payments of the

fees associated with each year of the term. Through such cloud subscription agreements, SaaS vendors are acting like traditional software vendors. They are looking to protect predictable revenue streams by motivating customers to sign fixed-fee contracts with upfront commitments with very little flexibility.

Ensure You Don't Pay for 'Air'

In many instances, these fixed commitments for specified numbers of users create the dreaded "shelfware" effect. Enterprises that are forced into upfront commitments end up buying more user software licenses than necessary. And of course, the on-premise software contract offers no relief in terms of reducing the number of licenses during the contract term. It's bad enough customers are not using all the user licenses or functionality they purchased and paying upfront compounds the problem.

This is no different than what happens in SaaS scenarios. *The only difference—and it is a big one—is that the enterprise does not own a license to walk away with and use later.* When an enterprise enters into a SaaS cloud subscription agreement, they are renting access to the functionality. Once the term is up, you must renew if you want to continue to have access. The renewal resets your payment obligations, often including an uplift to the pricing — and doesn't account for the enterprise previously **paying for air**.

In these cases, enterprises should challenge their various SaaS vendors to include the ability to scale up and down as needed during the term of the cloud subscription agreements. This means that as usage decreases, SaaS vendors should provide the customer the ability to reduce the commitment to align with actual need at that point in the term, with a corresponding reduction of the fees or a credit towards future usage.

Price Certainty Through Price Protections

SaaS cloud subscription agreements are often ambiguous regarding protections against price increases applied to any additional products and/or users added during the term. Enterprises, especially those that execute multi-year cloud subscription agreements, should not be susceptible to such increases. All SaaS cloud subscription agreements should include clear language stipulating the option to add additional product and/or user subscriptions at the upfront final negotiated price or even a lower price based on an overall volume increase.

Having price protections in place at the time of renewal (i.e., 3 years after signature) is critical. Under standard SaaS cloud subscription agreements, price increases apply at the end of the initial term when enterprises must renew. Contract language should either remove the ability to increase for a specified period of time or specifically limit or "cap"

When an enterprise enters into a SaaS cloud subscription agreement, they are renting access to the functionality. Once the term is up, you must renew if you want to continue to have access.

the price increase that the SaaS vendor may impose at renewal. In addition, customers should not be required to maintain a certain quantity of products or volume of users to receive the benefit of the committed price protection.

SaaS Vendor Responsibility upon Termination

SaaS cloud subscription agreements should clearly state SaaS **vendor obligations upon termination**. For example, SaaS vendors should provide transition services, including temporary hosting to ensure business continuity.

Another critical area of concern in SaaS contracting is data ownership and management. Standard SaaS cloud agreements are ambiguous at best. Data is usually stored on SaaS vendors' servers and behind their firewalls. *However, customers must retain full "ownership" and have access to their data at all times.* Specifically, companies must ensure they can obtain a complete copy of their data from SaaS vendors, upon written request.

Back-up, encryption, and data disposal processes should also be spelled out in advance in case of future litigation or termination.

At a minimum, upon termination, data should be returned to the customer in both the SaaS vendor's data format and a platform-agnostic format. Once a successful hand-off of that data has been confirmed, all customer data should be permanently removed from all SaaS vendor servers.

Lastly, customers must be fully informed if their data is going to be used by the SaaS vendor for internal benchmarking purposes.

All these requirements and scenarios should be covered in detail within SaaS cloud subscription agreements. Further, enterprises need to ensure that the security and privacy policies are spelled out clearly in the contractual documentation, especially as they relate to mandatory industry regulations.

Section 2

SaaS Cloud Subscription Agreements ≠ On-Premise Software Agreements

It's ironic that the contracting practices of SaaS vendors so frequently resemble more traditional on-premise software deals that helped make SaaS a popular alternative in the first place. But unfortunately, that is the reality and the reason more flexibility needs to be negotiated into all SaaS cloud subscription agreements. In some cases, it's simply a matter of ensuring that the on-demand flexibility enterprises expect from SaaS solutions is formalized and clearly stipulated in contracts.

Enterprises must ensure their cloud subscription agreements and relationships with SaaS vendors are structured in a way that allow them to leverage the considerable advantages of this 21st-century cloud delivery model. As the cloud and SaaS continue to gain traction in the marketplace, objective market intelligence and proven contract and relationship management approaches tailored to SaaS will only become more valuable.

When "On-demand" Really Isn't

Large legacy on-premise enterprise software vendors, like SAP, Oracle, and Microsoft, continue to push their "on-demand" SaaS cloud products into their customer base. To a large extent, these efforts are designed to counteract the competitive threat posed by the major SaaS cloud vendors like Salesforce, Workday, and ServiceNow. The same could also be said about pushing their customers to their new offerings around mobility, virtualization, AI and IoT.

Organizations considering the move to the cloud or any of these other emerging technologies must keep in mind that, unless they secure the right upfront pricing and they structure their contracts properly, their cloud experience will feel very similar to their experience with traditional, on-premise enterprise software.

If not careful, the alleged highly flexible "metered" and "usage-based" pricing model that comes with cloud subscriptions will include many of the same traps – like auto-renewals and required multi-year upfront commitments – as seen in more traditional on-premise software agreements. Whether you are dealing with cloud solutions from one of the traditional enterprise software powerhouses like SAP, Oracle, and Microsoft, or one of the large cloud vendors like Salesforce, Workday and ServiceNow, usage-based pricing can be not all that it seems. Below are a few important points to consider.

Most software vendors will position "flexibility" as the prime reason to make the switch from traditional on-premise license models.

Buying On-demand

The perceived on-demand nature of SaaS cloud subscriptions appeals to organizations as it implies the ability to spread out payments over time and as your users need access to the functionality. In fact, most software vendors will position "flexibility" as the prime reason to make the switch from traditional on-premise license models.

But more often, organizations must contractually commit to multi-year terms requiring upfront payments of fees for each year of the term.

Most SaaS cloud subscription agreements don't reflect a truly flexible, on-demand model. They are not structured for precision metering of actual consumption, rather, they look more like traditional, on-premise software contracts, with fixed fee payments for a specified set of products and a committed number of users. What's worse, the expected commitments are set in stone for multiple years, with obligations to make upfront payments of the fees associated with each year of the term.

This practice means software vendors, whether they are selling you a SaaS cloud product or a more traditional on-premise software solution, are still looking to protect a predictable revenue stream from their customer base.

Upfront Commitments

If software vendors insist on upfront commitments, organizations must push back for significant upfront discounts in return. Software vendors must be reminded that the positioned on-demand nature of the cloud and SaaS solution is a compelling factor in whether your organization is willing to adopt. If that benefit is diminished in any way, it may no longer be worth switching from an on-premise model. The software vendor's ability to present meaningful additional upfront discounting will go a long way in mitigating these concerns.

SaaS cloud subscription agreements also often lack volume discounting commitments. These agreements should include clear language stipulating the option to purchase additional

subscriptions at the upfront negotiated price until an established volume threshold is met and eclipsed, where at that point the go-forward price will be reduced given the organizations expanded volume commitment.

Renewal Price Protections

Having price certainty and protections in place come renewal time (i.e., when your subscription term ends) is also critical. Most cloud subscription agreements include the ability to increase prices at the end of the initial term or there is ambiguity around price protections, thus an organization could be completely exposed.

All cloud subscription agreements need to include language that specifically limits the vendor's ability to increase prices when it comes time to renew.

- There should also be a period in which there will be no increase in pricing. This is often harder to achieve but there is precedent for this level of commitment from vendors.

- The contractual language should not include conditions like 'increased volume' or 'adoption of additional cloud products' for the protection to be available.

It is always important to read the fine print because these types of conditions often show up after careful review.

Auto-renewals

Most cloud subscription agreements include default language around auto-renewals. This language should be removed from cloud subscription agreements and alarm bells should go off if software vendors are reluctant to do so. Software vendors, especially those previously mentioned, should be confident that the value received from their cloud offerings will lead their customers to renew by choice, not by contractual requirement or technicality (e.g., failure to notify the software vendor of cancellation within an allotted time frame).

The bottom line is that when an organization is considering a software vendor's cloud offering, it is critical to think as much about how they structure the subscription agreement as the exciting potential to improve the agility and speed of the business through cloud adoption and integration.

Once you've determined your overall SaaS cloud contract fundamentals, it's important to take it a step further to focus on your SLA agreements.

Section 3

How to Make SaaS Cloud SLAs Meaningful

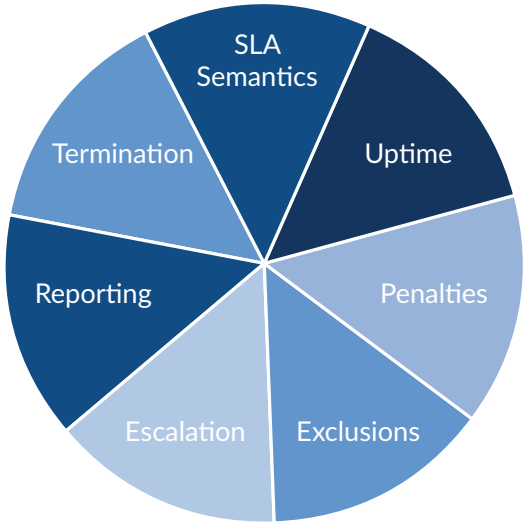
SLAs, or service-level agreements, are standard within the IT outsourcing landscape. As large enterprises have outsourced more IT functions – everything from application hosting, to application maintenance and support to IT help desk support – they have viewed SLAs as mini-insurance policies. The idea was to "guarantee" the chosen IT service provider would deliver the promised performance levels or face penalties (like credits) which would allow the enterprise to focus its attention and internal resources in other value-add areas.

But IT service providers may think of SLAs as something they simply have to do and must include in every master services agreement to reassure their customers. In some cases, they may not give SLAs much thought at all, using vague or generic language that doesn't match the customers' desired performance, outcomes and/or needs. That's why SLAs are often worth little more than the paper they're printed on, especially if there is no accompanying meaningful penalty structure.

Today, with more firms embracing SaaS and cloud computing models in general, IT executives are particularly eager to establish clear baselines for performance like those put in place with their IT service providers. SLAs may play an important psychological role in reducing the anxiety some enterprises may feel about adopting solutions that reside in the cloud.

Clearly, meaningful SLA structures should be a part of all master subscription agreements with all chosen SaaS vendors.

Ensure Meaningful SaaS SLAs by Considering:



SLA Semantics

First and foremost, enterprises need to move beyond boilerplate and standard "shrink wrap" SLA language. Most IT vendors provide contractual documentation that is heavily "vendor-centric." In many cases, SaaS vendors are reluctant to actually negotiate SLAs and will cite the difficulty in having custom SLAs and obligations for individual enterprises.

Uptime

Every SLA needs to have language that provides assurances relative to uptime. When addressing uptime requirements, the measurement period needs to be carefully considered and addressed. The longer the measurement period, the more diluted the effects of the downtime. The moment the downtime starts, the clock needs to begin ticking in terms of calculating downtime. If vendor servers fail, end users may lose access to critical applications and data, which could severely impact the business.

Penalties

Should the SaaS vendor fail to achieve the uptime requirements or guarantees, clear and specific penalties should be defined and enforced. IT vendors will usually push for penalties of free application time (i.e., additional use) but this is of little value to enterprises if they are dissatisfied with the service in the first place. This also would require the enterprise to continue to use the SaaS solution.

A better penalty structure should involve service credits that escalate as the length of downtime increases. It is simply not enough to have a structure with service credits; they must incentivize the vendor to act quickly. A nominal credit amount is not going to provide much relief and will certainly not offset the damage tied to not having access to the application for an extended period -- especially if it is a critical application. In fact, nominal service credits may make it more economical for the SaaS vendor to fail than to deliver in line with contracted terms.

SLAs are often worth little more than the paper they're printed on, especially if there is no accompanying meaningful penalty structure.

The willingness to accept significant service credits provides great insight into a SaaS vendors' confidence in the reliability of their own system and their willingness to stand by their cloud offerings.

Exclusions

Once an optimal SLA structure is in place, with clearly defined expected targets and meaningful penalties in the form of significant service credits, enterprises need to ensure the language does not also include significant exclusions to the right to penalties. IT vendors will undoubtedly look to include many exclusions to manage their overall risk. The more exclusions, the less meaningful the SLA structure becomes.

Escalation

In addition, there needs to be an escalation clause included within all contracts. Clear processes should be in place for resolving contractual issues, especially those associated with SLA adherence. Strong escalation processes around SLAs can be a critical element in establishing open communication, transparency and a healthy overall relationship with key IT vendors.

Reporting

SLA provisions should also stipulate that SaaS vendors provide monthly and/or weekly reports on key availability, continuity and performance metrics. There should be regularly scheduled SLA meetings to review this information.

Termination

Lastly, every SaaS cloud subscription agreement should include a provision that allows the enterprise to terminate for serious or continuous failure to meet established service level requirements. There should be no early penalties tied to terminating for SLA non-performance and the vendor obligations upon termination need to be clearly stated.

The bottom line is that SLAs are an important part of all SaaS cloud subscription agreements but only if the SLAs themselves are clear and the penalty structures behind them are meaningful. An enterprise's deeply discounted SaaS subscription price can turn out to be very costly if the application does not meet the expected level of availability.

Section 4

Stay Out of Security Breach Headlines

It seems like you can't go a day without reading a headline regarding yet another high-profile mass data and security breach. Security and data breaches are a concern for corporations, universities, individual consumers, and even the US government.

There is no question the risk of security and data breaches must be considered an extremely serious matter and remain top of mind at the executive and board levels within all organizations.

Much of the stories pertaining to security and data breaches have been tied to information accessed within cloud solutions or hosted websites. Given the current trend to adopt cloud solutions, it has become even more critical for organizations to ensure their agreements effectively address security and data breaches. The good news is, if done correctly and with the proper level of insight, there are ways to mitigate the risks associated with such breaches.

3 Key Areas to Effectively Address Security and Data Breaches

1. Security Measures and Protections

All organizations evaluating a cloud solution must fully understand the unique security measures and protections of the cloud vendors being evaluated. At the outset, it is important to get the cloud vendor's confirmation that their security policies and procedures adhere to necessary certifications (SAS 70, PCI Security). If your organization has specific security requirements, it is important to communicate these upfront with the vendors under consideration, and clearly identify them as a key component in your decision-making process.

It is no surprise that many cloud vendors will resist such requests, stating that in order to keep costs competitive, they need to standardize on security policies in a one-size-fits-all approach that applies to all customers. Therefore, the cloud vendor will claim they simply cannot customize the solution and

associated services to match unique customer security requirements. Nonetheless, we still recommend engaging in these discussions early in the evaluation process when you have the greatest leverage, as vendors may be willing and able to get creative in providing some level of flexibility that either addresses your unique security requirements or substantially mitigates your financial risk.

agreed upon period, usually within 24 hours. The written notification should include a detailed report specifically outlining how the breach occurred, which information and data was compromised, and what is being done to remedy the current security breach and prevent future breaches. The cloud agreement should also clearly identify the amount of damages available, and if possible be excluded from any limitation of liability provision, along with an ability to terminate the agreement for cause without any early termination penalty.

It is critical that your cloud agreement expressly states that your organization shall maintain ownership of and access to all information and data at all times.

Other security measures to address include the physical location of your data and where the cloud solution will be hosted. For example, some organizations may have regulatory requirements restricting them to U.S. locations only. The hosting and data location may also impact governing law and jurisdiction in the event of a dispute, so we recommend obtaining the opinion of legal counsel early in the sourcing process. Additionally, it is important to have clear and documented policies and procedures that govern who may have access to your organization's information and data.

Lastly, organizations must obtain from their cloud vendor expressly stated obligations regarding how it will resolve and mitigate damages should a security breach occur that may expose your organization's confidential information and data. At a minimum, the cloud vendors should be obligated to provide notice of all security and data breaches within an

2. Data Protection, Rights and Backup Obligations

It is critical that your cloud agreement expressly states that your organization shall maintain ownership of and access to all information and data at all times. This may seem like an obvious provision, but it is often overlooked and not included in the template agreement of many cloud providers. Additionally, it is important to ensure your agreement provides an obligation on the part of the vendor to provide a complete copy of all your information and data upon written request and in an agreed upon format acceptable to the organization. It is not uncommon for a cloud agreement to include an obligation on the part of the customer to pay a fee associated for the retrieval of such information and data, but we recommend

negotiating the removal of this fee, or alternatively, clearly identifying the fee within the agreement.

The cloud agreement should also clearly identify all backup schedules and policies. For mission-critical and highly sensitive information, it is important to ensure you obtain the cloud vendor's commitment to perform backups throughout each day. You should also have included an obligation for the vendor to encrypt the data and break it into pieces so that full files cannot be easily retrieved or reassembled if they are stolen. Such encryption should be provided at no additional cost.

Upon any termination of the agreement, there should be clear procedures for the timely return or retrieval of all your information and data in a predetermined format. This should include an obligation for the cloud vendor to certify that such information and data has been permanently deleted or removed from the vendor's servers.

Lastly, all organizations should have a complete understanding of how its information and data will be used by the cloud vendor. We recommend protecting your information from being utilized for the vendor's own purposes and benefit (i.e., mailing lists, marketing campaigns, selling to other vendors, etc.) that are not reasonably related to the vendor's ability to provide the service.

3. Data Center and Security Procedures Audit Rights

In keeping with the need to proactively ensure your organization is doing everything it can to minimize any potential risk of data and security breach exposure, all cloud agreements should provide an organization the right to perform periodic audits of the cloud vendor's data centers. The scope and breadth of such audit rights should cover the vendor's data security controls, processes, and procedures. The organization should have the ability through such audit rights to ensure compliance with the detailed security provisions found within the cloud agreement. An organization's ability to exercise the right to conduct such an audit is one of the best ways to hold the vendor accountable to their stated security obligations and to proactively assess any potential security vulnerabilities. It is apparent that having the right to conduct an audit is an effective means to mitigate the risks associated with security breaches.

Unfortunately, it is highly unlikely the risk of data and security breaches are going away anytime soon. The key is making sure your organization is doing everything possible to ensure your risk exposure is appropriately mitigated. By addressing the issues outlined early in the selection and negotiation process, you will be on the right path to keeping your organization from being part of a news security breach headline.

About the Author:

Adam Mansfield is the Practice Leader of the Microsoft, Salesforce, and ServiceNow advisory services at UpperEdge. Adam is considered a thought leader in cloud subscription agreement negotiations and has over 15 years of experience negotiating software, system implementation, cloud computing, and data center agreements that ensure optimal deal constructs and significant savings.

Contact

Carole Jacques

Director of Marketing

617.412.4313

184 High Street, Suite 502

Boston, MA 02110