

IMPORTANT NOTES:

This material is only for REFERENCE. It may be IP protected and should NOT be distributed or circulated without the consents of the author.

Top 10 SaaS Terms to Negotiate That Avoid Putting Your Budget and Business at Risk

Published 26 April 2021 - ID G00722426 By [Jo Liversidge](#)

<https://www.gartner.com/document/4000965?ref=authrightrec&refval=4009001>

Sourcing, procurement and vendor management leaders are often under pressure to negotiate an increasing volume of SaaS contracts quickly, limiting the attention given to negotiating key terms. Use this checklist of the top 10 SaaS terms to evaluate and negotiate to reduce risks and optimize costs.

Key Findings

- Sourcing, procurement and vendor management (SPVM) leaders brought late into the negotiation process too often find that stakeholders have at best negotiated only the price of the initial deal.
- Risks are often hidden in referenced URL linked terms, such as security policies or SLAs, which vendors can change unilaterally.
- Failing to consider a viable, realistic exit strategy before contract signature can lead to vendor lock-in and significant, unbudgeted costs.

Recommendations

SPVM leaders negotiating SaaS contracts who need to gain traction with CIOs and senior stakeholders, should:

- Negotiate renewal price increases of no more than 3% to 5%, negotiate hidden costs (such as sandboxes), and negotiate a pricing model that suits the organization's demand plan.
- Incorporate key terms, such as service descriptions, support levels and security policies, into the contract, along with "not to diminish" wording. Don't rely on URL links.
- Negotiate exit-related provisions, such as data extraction clauses, and transition assistance to minimize migration costs and risks.

Introduction

CIOs and business leaders pressure SPVM leaders to complete urgent SaaS contract negotiations quickly, with reducing costs and mitigating risks as key priorities. However, many SaaS providers represent key terms as non-negotiable. This means that too many SaaS contracts are being signed "as is," leading to unbudgeted costs throughout the contract term and at renewal. Additionally, terms about service and exit are not documented, leading to greater lock-in risk and additional — often prohibitive — costs on exit. In a recent Gartner survey 43% of respondents answered that SaaS deals were difficult to negotiate. Compare this to only 29% stating that on-premises software was difficult.

SPVM leaders frequently ask, "What are the most important terms we need to negotiate in SaaS deals?"

To answer that question, this research provides a concise overview of the top 10 SaaS terms. It is not an exhaustive list of terms. It represents the top 10 key terms that Gartner analysts believe are the most relevant to SaaS. Use it as a way to get traction with senior stakeholders and CIOs and to highlight the main costs and risks of SaaS contracts. A one-page slide of these top 10 terms is included for you to use with your internal stakeholders.

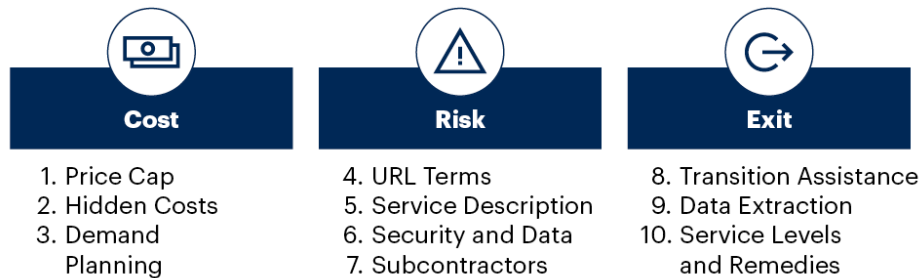
Also attached is a slide deck, with a slide for each of the ten SaaS terms, for you to use internally within your organization.

Top 10 SaaS Terms To Negotiate

The negotiation of these top 10 terms will not apply to all SaaS contracts. It is essential to take the criticality of the services into account and to plan the negotiation accordingly. The top 10 terms can be grouped under the three headings of cost, risk and exit, as shown in Figure 1. Not all of these terms will be relevant to all SaaS contracts or to your environment. However, at the very least, you should consider each term against the application's criticality to your business.

Figure 1. Focus on the Top 10 SaaS Contract Terms

Focus On the Top 10 SaaS Contract Terms



Source: Gartner
722426_C

Gartner

This high-level checklist complements Gartner's more detailed research and Tools/Toolkits to assist those analyzing, prioritizing and negotiating the specific terms and conditions of SaaS contracts. That detailed research includes [Tool: Checklist for Negotiating Optimal Cloud SaaS Contract Terms and Conditions](#) and [Toolkit: Negotiate Favorable SaaS Contract Terms Utilizing a Standard Amendment](#) as well as a number of vendor-specific ones (see Note 1).

Gartner does not provide legal advice or services, and its research should not be construed or used as such. Work with your legal counsel to incorporate the recommendations herein using contract language customized to meet your internal legal and business requirements.

Analysis

Negotiate Renewal Price Caps, Potentially Hidden Costs and a Pricing Model That Matches Your Demand Plan

1. Negotiate a Renewal Price Cap to Ensure SaaS Contract Costs Stay Within Budget

This is the most important commercial contractual term. SaaS is a subscription, with typically high levels of lock-in, which leaves clients exposed to significant price increases on renewal, if not negotiated.

Although many vendors do not have standard terms related to the limit the pricing can increase on a renewal term (renewal uplift cap), many providers will negotiate this cap as part of the initial contract discussion. (For a sample list of vendors' terms related to this, see Note 2). Ideally, the renewal uplift cap should be a one-time uplift at the date of the renewal, not an annual uplift that is set at a maximum of 3-5%, or CPI, whichever is lower.

Generally, larger SaaS vendors will offer fixed pricing for the initial term of the contract, while smaller providers may include an annual uplift in a multiyear deal. In contracts with annual uplifts, a cap that is the lower of 3% or consumer price index (CPI) is more appropriate. Some Gartner clients have had success negotiating no, or a lower, uplift on first renewal to give a longer term of flat pricing as part of an initial deal. This then reverts to a standard agreed cap for the second renewal onward. There are a few larger vendors, such as Microsoft and Workday, that, despite benefiting from a multiyear commitment, sometimes ramp a contract discounting. This means the highest discounts in Year 1 and decreasing discounts over the term of the contract, with the lowest discount in the final year. This final year cost is the all-important cost that will form the basis of your renewal pricing, so that ramped cost profile will likely turn out to be more expensive in the longer term and needs to be thoroughly analyzed.

2. Proactively Identify and Negotiate Any “Hidden” Fees That May Apply to Your SaaS Deal

SaaS providers present pricing as “all in,” including capabilities, patches, new versions, hosting and support services. However, the vast majority of SaaS products have limitations (or “allowances”) attached. Not all providers make these limitations transparent. These limitations often sit in the referenced “documents,” “service descriptions” or URL links. For example, storage (file and data), custom objects, API calls, page views, connectors,² contacts and sessions, if exceeded, will require customers to pay incremental fees. In addition, providers may not always technically restrict your usage. The restrictions may only be contractual. For example, you may use more storage than your allowance or send more API requests than included within the core products.

It is imperative to investigate all potential additional costs, ideally at the vendor selection stage. You need to proactively request this information from providers during sourcing activity. Secure details of all applicable limitations and of the costs of purchasing incremental units. These costs should be negotiated in parallel with the subscription fees. Otherwise, you will pay premium (list) pricing for any overages that occur after contract signing.

Sandboxes and premium support are the two biggest potential additional costs when implementing SaaS solutions.

Sandboxes: Many organizations need at least one test and development environment (“sandbox”). For complex implementations, such as ERP, it is not unheard of for clients to need multiple extra sandboxes. Many providers include one sandbox with the product purchase,³ but charge for additional sandboxes. For example, this extra charge can be 30% of the net subscription fees.⁴

Work with stakeholders to size the sandbox requirements. In parallel, investigate how many, if any, sandboxes are included in the base subscription fees, and then negotiate the costs of extra requirements.

Premium Support: A certain level of support is included in the subscription fees. However, this support may be very basic, especially if the provider offers a higher level of support for an extra fee. For example, SAP offers an enhanced support level called “Preferred Care,” which retails at 20% of net fees.⁵ This fee is negotiable with SAP and others, such as Salesforce, if you have good leverage, such as before you have committed to the solution. (For details, see [Tool: Critical Terms to Negotiate in Your SAP SaaS Contract](#).)

Although many premium support offerings include faster incident response times and other improved service levels, they do not necessarily offer any better remedies for underperformance. You need to investigate what support services are included in the subscription fees. Then, you need to determine whether that SaaS provider offers varying levels of support and at what cost. If you identify a higher level of support and negotiate the associated fees before signature, you can potentially reap significant savings. We have seen savings of 50%.

3. Negotiate Flexibility Into the Pricing Model and Contractual Terms to Align With Your Demand Plan

Consumption-based pricing is often assumed to be synonymous with cloud offerings. However, most SaaS providers expect a multiyear commitment for a set quantity — which you will pay for regardless of whether you use 100% or 0% of the capacity. Provider contracts will typically allow you to add units during the term, but not reduce them. For some providers, this situation is starting to change. Gartner has seen evidence that, where customers are able to show a business case for a consumption-based model, some vendors are starting to meet this requirement at least part way.

Work with business stakeholders to analyze projected consumption patterns. If the demand is variable, then proactively request consumption-based pricing for a portion of the contract. Consumption-based pricing fits some scenarios better than others. For example, retail, utilities and financial services are prime candidates to require some flexibility in commitments. Some vendors, such as Microsoft, offer contract vehicles that enable greater flexibility.⁶ As with most terms, you have more leverage to achieve this provision if you negotiate before the selection of the provider. See the attached “SaaS Consumption Models” slide, which shows various scenarios.

Negotiating product exchange rights (also referred to as product swaps) can also give an element of flexibility into a typically inflexible contract and help to minimize shelfware.

Incorporate Vendor URL Terms Into the Contract, Along With “Not to Diminish” Wording

4. Incorporate Detailed Service Descriptions for All Products in the SaaS Contract, Ensuring All Limitations Are Clearly Documented

Very few SaaS providers include a description of the services in their contracts as standard. The inclusion is something that needs negotiating. Providers change capabilities and product entitlements over time. Some providers, such as Salesforce, change the names of products on a regular basis. Therefore, it is important to have a record of what you are purchasing, over and above the list of product names on the order form. Some providers have service descriptions readily available on their websites. Other providers have data sheets, which can vary enormously in their usefulness of information.

It is important that you have a detailed description of the capabilities for the products you are purchasing and that this description is included in the contract (usually as an exhibit or appendix). If it is not possible to attach the service description, then it is imperative you reference the document relevant on the date of signature, including date and version number. You should also negotiate a warranty that the services and any associated entitlements will not materially diminish during the subscription term.

5. Research and Incorporate Other Key URL Terms Into Your SaaS Contract to Mitigate Against Decreasing Support Levels and Security Standards

In addition to descriptions of services, SaaS providers incorporate many other key documents via reference. The reference is often a URL link to a plethora of additional information, including, but not limited to, product terms, support descriptions, SLAs, security policies, data protection addendums/agreements and disaster recovery policies. Providers can amend these additional terms, and frequently do so. Some providers do warrant that they will not diminish certain terms, such as security policies and support descriptions, during the subscription term. Other providers, such as SAP,⁷ reserve the right to potentially materially reduce functionality, but allow customers to terminate the service within 30 days of SAP's notification if they can prove a material reduction. This remedy, however, is not desirable, inexpensive or pragmatic.

You should negotiate the incorporation of key documents as exhibits to the contract, as the full baseline of services, including support services, SLAs, security standards/policies and disaster recovery documentation, and negotiate that these will not diminish during the subscription term. This list will vary depending on the criticality and type of services being purchased.

6. Thoroughly Review Terms Related to Security and Data Privacy to Ensure Compliance With Your Requirements

Data security and privacy cannot be governed exclusively through a contract. With SaaS providers, the contract terms related to security and privacy are variable. The terms may be available via URL links or,

especially in relation to security, only “on request” by the customer to the provider. This lack of accessibility presents risks. Although the provider is responsible for security of the data, you are accountable if adequate security is not provided. Often, there is less than optimal transparency about how robust that security might be.

It is imperative that SPVM leaders investigate all security requirements before they select a SaaS vendor. If the provider does not currently have, for example, a certain certification that is imperative for your business application, then do not expect the provider to secure that certification just for your business. This is why it is important to review security provisions in detail with business stakeholders during selection. There is evidence of some providers adapting their terms when a regulatory reason would otherwise cost them a client’s business. For example Microsoft has a standard amendment (M248) to allow regulated financial services customers certain audit rights. Gartner recommends that you aim for the annual completion of at least Service Organization Control (SOC) Type 2 audit reports by your provider. Alternatively, aim for compliance with the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and 27002 standards. You should also negotiate the explicit right to terminate the contract should the audit reports reveal severe risks or show that risks are not mitigated within a reasonable time.

Data privacy legislation varies between industries, between countries and even within individual countries. It is imperative that legal counsel is involved to ensure data privacy terms are suitable for your unique set of circumstances. The European General Data Protection Regulation (GDPR), and increasingly other privacy legislation in other countries,⁸ adds another layer of complexity for any organization, regardless of geography, that deals with the personal data of EU citizens. Most large providers have a standard data processing addendum, and you will probably need to request it. However, some providers may not meet all your organization’s privacy requirements. For example, a SaaS provider may not be able to guarantee that your data will be stored or processed within a certain region or country. Include data security and privacy policies in exhibits to the contract, and refer to those exhibits in the relevant contract clauses.

7. Ensure That Your SaaS Providers Take Responsibility for Their Subcontractors

Many SaaS providers use subcontractors, including other cloud providers. For example, SaaS providers may leverage Amazon Web Services (AWS) or Microsoft Azure. Therefore, it is imperative that the SaaS provider take responsibility for those subcontractors, and that the terms of the SaaS provider’s contract govern over all others. In some contracts, SaaS providers are not responsible for any failings from subcontractors or infrastructure providers. For example, if you were concerned with the IaaS performance, you would have to negotiate with the IaaS provider. This arrangement is unviable, since, typically, you would not have a relationship or leverage with that provider.

Therefore, negotiate that subcontractors must abide by all negotiated terms. Ask upfront if and how subcontractors are involved in the provision of the service. Be clear on who the subcontractors are and on what elements of the service they are providing. If those elements are critical, then ensure you have

performed an analysis of the risk of the solution. Include a list of subcontractors as an exhibit to the contract. The contract should also include a clause for changes in subcontractors. In the event there is a planned change in a subcontractor, the provider should give at least 60 days' notice. If the provider fails to give this notice, or if the customer deems the proposed change unfavorable, then the customer should (at its sole discretion) be able to terminate the agreement without penalty or obligation.

Negotiate Data Extraction and Other Exit-Related Provisions to Future-Proof Your SaaS Contract

8. Include Key Service Levels and Appropriate Remedies for Critical SaaS Applications

SLAs for SaaS are often limited to just system availability, and not all vendors offer even this. Because termination for convenience is not standard for most SaaS providers, and never standard for large providers, having explicit remedies for poor performance in your contract is especially important. These should ideally extend beyond system availability alone. Other service levels to consider are a downtime definition, incident response times, incident resolution times, disaster recovery objectives and security standards. Some providers do include these for some products. For example, Zendesk “guarantees” a one-hour, global first-reply time to English-language inquiries for 95% of requests (for certain editions).⁹ Although SaaS providers won't always include service-level metrics beyond those offered as standard, there is evidence that some providers will negotiate some terms. For example, an improvement to the service credit value may be negotiable.

Negotiate meaningful financial penalties by incorporating escalating tiered credits, up to 100% of monthly fees, for missed service-level targets. Gartner recommends that you adapt your negotiation demands for service levels to the criticality of your application. For example, for low-value and noncritical applications, a longer incident response time and lower or no service credits may be appropriate.

A Termination Right Is a More Powerful Weapon in Your Armory Than Service Credits for SaaS Providers

Gartner has seen some customers with good leverage negotiate a right to terminate at any point in the future if the agreed service levels are missed for any three months in a rolling 12-month period. This type of clause has advantages over the standard “termination for cause” wording. For example, it gives you the time to plan and manage your exit from the underperforming vendor. A termination provision that is time-bound is not usually a realistic threat if you have multiple integrations into other systems that will take many months to transition. For more details on SaaS SLAs,

9. Do Not Assume That, Without Negotiation, Your Data Will Be Easy or Free to Extract When You Need It

Terms related to data extraction upon expiry or termination of a SaaS contract vary enormously between providers. Some SaaS provider contracts state that the provider can delete all data on expiry of the contract.⁹ Other contracts give you a set amount of time after expiry or termination to retrieve your data before the provider deletes it (typically 30 or 60 days). Many contracts state that you must proactively submit a request to retrieve your data. In addition, many SaaS contracts are silent on the format of the data, and almost all are silent about any associated potential costs.

Therefore, it is important that terms related to data format, extraction and any costs are set out explicitly in your SaaS contract. You should negotiate sufficient time to retrieve your data after the expiry or termination of the contract (typically 60 to 90 days, but this period could be far longer for system-of-record applications). In addition, extraction rights should ideally be automatic, not by request. Moreover, you should be able to extract the data in a mutually agreed format set out in the contract.

10. Negotiate Transition Assistance and Extensions to Subscription Services

SaaS has a notoriously high degree of lock-in, especially for larger enterprises with widespread integrations into multiple systems. However, it is possible to future-proof your contract and plan for a possible exit to some extent. This can partly be accomplished by effectively “buying time.” Very few SaaS contracts explicitly detail what happens on expiry, with the exception, in some cases, of some mention of data extraction.

Unless the SaaS application is only for a short-life digital project or proof of concept, you may at some point transition to an alternative SaaS provider. For most scenarios, you should negotiate the option to purchase an extension to the term of your subscription, for a period that is less than the one to three year minimum usually required at renewal. You should also negotiate a professional services rate card with the SaaS provider so that, if required, you are not trying to negotiate these at the end of the agreement with no leverage. In certain scenarios, such as your termination of the contract due to provider breach, it is reasonable to expect certain assistance from the provider free of charge. This needs to be negotiated and set out explicitly in the contract.

Evidence

¹ Gartner’s Sourcing, Procurement & Vendor Management 2020 Survey: Results presented are based on a Gartner study conducted to identify the greatest challenges SPVM leaders are facing today when negotiating with and managing technology vendors. This primary research was conducted online in September and October 2020 among 279 respondents in North America (n=130), W. Europe (n=84) and APAC (n=65). When asked the question, “How easy or difficult was it negotiating these technology deals over the past year?” 43% of respondents said SaaS contracts were difficult, which was higher than on-premises (29%) and IaaS (33%).

² The reclassification of SQL, Azure and Dynamics 365 connectors from Standard to Premium can lead to a 50% to 200% increase in license costs for customers using Power Apps prior to October 2019

³ Oracle includes one nonproduction environment in addition to a production environment for most of its products. Additional environments are chargeable. Salesforce has several types of sandboxes, and the different types and quantities are dependent on the edition of Salesforce you are purchasing. For example, unless you are buying the highest edition of Sales Cloud or Service Cloud, your base SaaS cost will not include a full-copy sandbox.

⁴ Salesforce Add-On Pricing: The list price for a full copy sandbox from Salesforce is 30% of net subscription fees.

⁵

⁶ Microsoft offers more flexibility than other large SaaS vendors. Under an EA, customers can true down subscriptions on the anniversary date of contract signature. Further flexibility is offered through cloud solution providers (CSPs) via a pay-as-you-go model to fit most organizations' needs, such as a farming customer with seasonal workers. See Choose the Right Agreement Prior to Your Next Microsoft Negotiation for more details.

⁸ For example, Law 13.709 of Brazil is the General Law for the Protection of Personal Data or, in Portuguese, the Lei Geral de Proteção de Dados Pessoais ("LGPD"), and was sanctioned in August of 2018 and came into force in 2021.

⁹ "Zendesk Support," Zendesk.

*** Attention: research are originally in English and I have translated it into Chinese by Google Translate as instructed by Peter. In case of any discrepancy between the English version and the Chinese version, the English version shall prevail.*