Real experts.
Real data.
Real savings.

WHITE PAPER

Stop Overspending on SaaS

A Guide to Contracting and Vendor Management

SaaS is no stranger to the modern IT enterprise portfolio. But, the evolution of SaaS and its impact on the business is far from over. As enterprises embrace SaaS for their most critical business applications, vendor contract negotiations have become the front lines for overcoming traditional objections to cloud-based software deployments – including security, performance and total cost of ownership. It's also become ground zero for overspending.

In the past decade, software as a service (SaaS) has transformed enterprise IT and continues to undergo rapid growth. Vendors, ranging from "old guard" players like Microsoft and Oracle, to pure-play vendors like Salesforce.com, have flooded the market with cloud offerings that promise to deliver high performance, ease of management and affordability.

To fully realize these benefits, buyers must apply extra caution as they navigate the purchasing process – specifically within contracting. There are several areas of the SaaS contract that are prone to hidden costs and to the risk of insufficient recourse in the event of poor performance, security and service levels. At a minimum, buyers should ensure the following areas of their contract are ironclad:

Users & Functionality

Get rid of minimum purchase clauses. Buyers should not fall prey to requirements to buy a minimum number of licenses (or have a minimum number of users) over the term of the contract. This will prevent you from reducing the number of users in the event you have to downsize business operations, cut staff, etc. For example, a company may need 500 users while the economy is strong – only to cut its user base to 150 in uncertain times. Without a clause that protects your right to reduce your number of users, usage and/or functionality, you can easily be locked into inflexible spending – negating one of the most highly touted SaaS benefits.

On the flip side, companies should require vendors to specify their ability to ramp up new users/usage quickly. What happens if your company takes on a major client or acquires another company? How quickly can your SaaS-based business application adapt? If a vendor can't support a major increase in users, then a company needs to evaluate other vendors. This must be specified in the contract – not just in sales talk.

By 2020, IDC estimates half of all new business software purchases will be of service-enabled software and cloud software will constitute more than a quarter of all software sold.

Data Protection

One of the first things a company should do when procuring a SaaS solution is establish data ownership. This includes who owns the data, as well as the data migration procedures and costs. Many companies subscribe to a SaaS solution assuming the data migration and ownership costs will be incurred by the vendor. That's not always the case and, depending on how the vendor works, can add another cost and complexity layer to your SaaS purchase.

Another facet of data protection is disaster recovery and backup. How a vendor stores, backs up and continues service in the event of a crisis/disaster is extremely important. Because your data will reside in a third-party data center, your contract should clearly communicate the vendor's disaster recovery and business continuity capabilities. This includes specifying how often data is backed up, where backup is stored and so on.

Lastly, companies should make sure data confidentiality is addressed in their SaaS vendor contract. SaaS is based on a multi-tenant architecture where a vendor stores multiple clients' data at a single location. Ensuring this data is protected and kept confidential is key.

Upgrades & Renewals

Many companies assume upgrades and renewals are a non-issue in SaaS contracting. While most SaaS vendors don't charge for upgrades, don't assume they're free. Confirm the cost in your contract. Additionally, be sure to address renewal rates in your contract by inserting language that limits or prevents renewal rate increases. Not doing this empowers your vendor to enact unreasonable rate increases once your contract is up for renewal.

Performance

When transitioning from an on-premise to a SaaS model, you are consequently outsourcing performance quality assurance. Therefore, you need to determine service level guarantees and performance metrics in your contract. These should address application availability uptime, performance monitoring, security, support response time and help desk accessibility (among others).

Buyers should also define grounds for termination for unacceptable performance. If there is a failure to meet certain service level agreement (SLA) requirements, buyers should specify the solution (e.g. SLA credits). This is of increased importance for security performance metrics, where compliance and brand trust is on the line.

Finally, buyers should specify termination costs and data transfer guidelines. Should you choose to terminate your vendor agreement, you need to understand the costs of doing so beforehand. Specify these costs, as well as data transfer costs and procedures, up front in the contract.

The SaaS contract is full of opportunities to overspend and underperform. Getting the most out of a SaaS investment is directly tied to how well companies understand these pitfalls and can enact strategies to avoid them.

Vendor Health, Risk Assessment & Auditing

Demand and perform due diligence on vendor health. Companies should conduct a diligence check on the vendor to determine financial health, use of subcontractors/third-parties, etc. This includes conducting reference checks of other clients who are in the same industry. SaaS may be pervasive across today's enterprise ecosystem, but the industry is still young. Companies should select vendors that understand not only the challenges of SaaS delivery, but the challenges and key business processes of their specific industry.

As part of your due diligence, you should ensure that your vendor can meet any legal and e-discovery requirements set forth by your clients, partners or industry. Certain industries have specific regulations about data, email, what should be stored, for what period of time, etc. Include a right to audit clause in your contract that allows you to audit the vendor's facility. Due to multi-tenancy, the usual forms of audits may not be possible; therefore, these requirements should be established beforehand.

Service risk management has become increasingly important as companies further understand the business continuity risks associated with the SaaS delivery model. For this reason, thorough risk assessment and analysis should be carried out as companies evaluate vendors. For example, what is your risk tolerance to down time? What would happen to your operations if you were down one day a week? One day a quarter? How can you mitigate those risks? The combination of contractual requirements (such as SLAs) and smart vendor selection will best serve your business operations.

Managing Your SaaS Vendor for Long-Term Savings & Protection

Saving opportunities go beyond the contract phase of any vendor agreement. How you manage your SaaS vendor is directly related to your overall spend. There are three key areas that you should focus on to calibrate your vendor relationship for long-term savings and data protection:

- Have a transition assistance clause: At some point in time, you will switch vendors. Save yourself the cost and headache of a painful switching experience by including a transition assistance clause in your agreement. Ask your vendor to provide support to export data, document interfaces and customizations that you will need to share with a new vendor.
- Negotiate renewal rates: Renewal rates should always be negotiable…no exceptions. Demand that any rate increases be negotiable as part of your contract specifications, and be sure to establish contractual limits on rate increases as a fail-safe.
- Enforce SLAs: As with all software, SLAs should be measurable and enforceable. Stay on top of your vendor and make sure they are meeting all performance metrics and service level requirements. When performance is subpar, enact the penalties specified in your contract. You've outsourced a lot of control to your vendor – don't let them abuse or misuse it.

Conclusion

Buyers should create and execute a targeted cost management strategy for their SaaS investments. This involves arming themselves with protection against the cost, contractual and performance-related pitfalls that have haunted many SaaS buyers. Through a long-term cost comparison before the purchase, contract-driven cost management tactics and post-contract spend management, companies can improve the performance of their SaaS investment and optimize total cost of ownership.

In some ways, SaaS procurement still represents the Wild West of IT spending – where transparency, standards and visibility have yet to be normalized. Insight into market pricing data, contract pitfalls and vendor flexibility will ensure that a company's next SaaS investment is optimized for performance and savings.

ABOUT NPI — NPI is a spend management consulting firm that protects companies from overspending in three cost categories where pricing is opaque, complex and inconsistent – information technology, telecommunication and transportation. Using price benchmark data and vendor-specific cost reduction expertise, NPI helps clients assure that each purchase is priced at or below fair market value and program selection, licensing and business terms are cost-optimized. Reviewing more than 14,000 purchases annually, NPI provides objective oversight for billions of dollars of strategic spend for its clients. To learn more about how NPI can help your company start saving today, visit www.npifinancial.com or call 404-591-7500.