COMITY IN THE CLOUD

THE BENEFITS OF SECURING A BALANCED CLOUD SOFTWARE LICENSE AGREEMENT

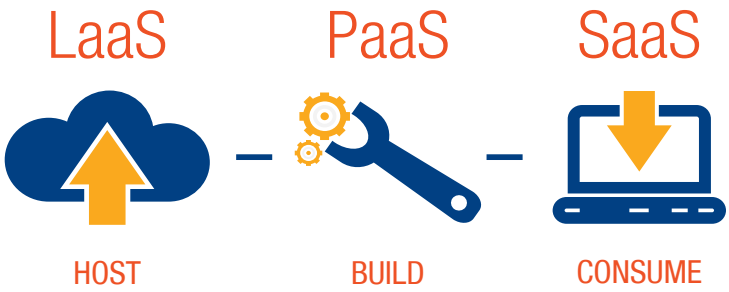
Comity (n.): courtesy and considerate behavior toward others

Negotiating and securing a specific Cloud Software License Agreement when purchasing systems from a Software-as-a-Service ("SaaS") or a "Cloud" [1] vendor is essential in protecting both parties in this digital age. The common "one size fits all" contract alternative doesn't address the true context of the Cloud vendor relationship with commercial real estate property managers, or its effect on the terms and conditions of the deal. This paper identifies common contracting problems; outlines the unique nature of Cloud software and licensing; and provides important guidance for negotiating licensing terms.

THE "STANDARD" AGREEMENT PROBLEM

To better illustrate the issues unique to Cloud vendor relationships, the scope of this paper is confined to a business-to-business relationship. It addresses the circumstance where one party comes to the bargaining table with a "standard" agreement to use as a template for establishing a relationship with a Cloud software vendor. The drafting party (usually the client) assumes that the existing agreement – appropriate for one service – must be appropriate for the new software relationship, save a few small changes such as pricing and a description of the deliverable.[2]

The impetus for using a standard agreement is obvious – the drafting party is trying to quickly come to terms on an "approved" services contract and avoid having to incur expensive attorney's fees or delay. What this approach ignores is the unique set of conditions, obligations, risks, challenges, and consequences attendant to a Cloud-based software relationship – all of which must be addressed in the agreement. When negotiating contracts of any kind, it is critical to fit the terms and conditions of the agreement to the subject matter of the deal. Professional Cloud vendors will have an appropriate Cloud Software License Agreement available for use which will include the client and vendors protections described below.



THE UNIQUENESS OF CLOUD SOFTWARE RELATIONSHIPS

Cloud software takes many forms, including application software, infrastructural software and platform-based services. "SaaS" provides applications on-demand enabling users in different locations to access it without installing anything on their computers, other than a standard browser. Infrastructural software-as-service ("IaaS") is a virtual computer accessed through the cloud, providing core computing services such as processing and data storage without the need to buy and setup a datacenter. Platform software-as-service ("PaaS") is a complete operating system hosted via the cloud. These "Cloud" services present unique issues regarding location, control, ownership and cost –all of which must be addressed in your software license agreement.

---

[1] "Cloud" and "SaaS" are thought to be synonymous terms of art; however they are not identical. "Cloud" is a catchall term for many forms of software-as-a-service. It is a figurative term reflecting the means through which these services are reach their users. Public or private Cloud generally refers to remote systems that serve many businesses through redundant computer systems designed to scale easily as their clients' businesses grow.

[2] Also avoid the "Duel Paper Problem" where both parties execute in a single document for their respective agreements and never achieve acceptance of either set of terms and conditions. Without specific agreement on terms, the court will resort to making the agreement for both parties under common law principles.

In contrast to traditional software, Cloud-based systems are hosted and maintained at locations remote from the client business, by third parties – either the vendor itself or a third party with which the vendor has a managed hosting relationship. Management of those systems; the underlying software, and the data managed by that software, is outside of the direct control of the client business. The third party Cloud vendor owns the software and systems and licenses access to those systems to the client under a "software license agreement." The client owns the data. The cost of those systems is borne entirely by the vendor which leverages the cost over many client relationships and earns back that cost, plus a profit, over a long-term relationship with each client. Hence, the nature and economics of the relationship are very different than with a traditional software vendor or typical service provider. The client needs to consider issues regarding system access; data security; data ownership; and data control when negotiating an agreement with a cloud software system vendor. Each are addressed below.

> ***"The client needs to consider issues regarding system access, data security, data ownership, and data control when negotiating an agreement with a cloud software system vendor."***

ACCESS AND THE SERVICE LEVEL AGREEMENT

We have all experienced the frustration of interrupted Internet service. The nature of the Internet makes it inherently vulnerable to system outages and system unavailability. System access and unavailability can be caused by many conditions – client business service failure; Internet Service Provider ("ISP") failure; mobile device failure; Cloud vendor system failure; or malicious causes like denial of service attacks.[3] Strong SaaS license agreements differentiate between these causes of failure and provide the client with differing levels of protection and compensation within a "Service Level Agreement" ("SLA").

Well-crafted SLAs define differing causes of system unavailability and provide for client protection when a problem is caused by the vendor, or defray responsibility when they are not. When a vendor's system fails, a typical SLA provides the client with a credit for its license fee – usually an amount in proportion to the level of interruption. In extreme cases, when the system is down for long periods, the SLA will provide the client with a monetary award or the right to terminate the agreement.

Most SLAs warrant 99.99 percent uptime, or system availability. Consequently, professional Cloud vendors have highly redundant systems and reliable failover [4] procedures in place to maximize access and minimize downtime. Cloud License Agreements with appropriate SLAs are the bulwark of a successful Cloud relationship and cover the gamut of conditions, causes, circumstances and remediation measures. Balanced SLAs preserve the economic benefit to both contracting parties while taking the realities of the Internet into account.

DATA PROTECTION AND OWNERSHIP

SaaS systems generally involve large quantities of data – activity data, contact data, performance data, asset-related data, and the like. While a "standard" contract generally includes protection respecting data and other confidential information, the issues are very different in the cloud – and vary for personal and non-personal data. While both a service contract and software license agreement address confidentiality, the "standard" service agreement fails to include provisions for limiting access to confidential information; for creating and maintaining back-ups of data; for providing continued access to data over time; and for providing the owner with ultimate control over its data.

Data generated during use of a Cloud Service is generally the client's data, unless the agreement specifies otherwise. When negotiating an agreement, ensure that the agreement is clear about data separation and establishes the proper ownership rights, access protections and controls. You may wish to shield your data from outside exposure; restrict access only to authorized individuals; protect the data from loss or transfer; and certify that when the relationship is over, you can obtain a copy of your data. There may be costs associated with these measures, but a well-crafted Cloud Software License Agreement should include language that addresses these issues and outline the costs associated with back-up and transfer.

---

[3] An attempt to make a network resource unavailable by saturating the target machine with external communications requests leading to server overload, system slowness or even failure.

[4] "Failover" is a set of automated procedures designed to transfer the load and operability of a system from one set of machines to another while minimizing downtime and data loss.

Many cloud vendors "anonymize" [5] client data and aggregate it with similar data from other clients to establish market standards, create collective thresholds, or establish important trends. This generally presents no risk to the individual client, and it is usually in each client's interest to release its data for that purpose. For example, collective anonymous performance data can be aggregated from many like organizations to set a general market standard against which the client's actual performance data can be compared. Market comparison helps each individual client to determine how it is performing against the general market without exposing its identifiable data to its competitors. Well-crafted Cloud License Agreements provide for data anonymity and aggregation while providing the client with access to collective information as part of the contract.

INSURANCE IN THE CLOUD

Insurance requirements outlined in standard agreements typically address physical concerns such as access to property where the service it to be performed, workers' compensation for injuries that may occur on premises, physical harm, or automobile-related risks. While these "general liability" concerns are relevant to most service-related contractual relationships, they do not address the specific issues and potential claims that arise from a Cloud software relationship.

Cloud software systems involve digital media and information. Software's easily accessible, reproducible and transferable nature presents unique issues regarding theft, copyright protection, and reliance. A Cloud system client should require the Cloud vendor to carry Errors and Omissions ("E&O") or Professional Liability insurance. "E&O" insurance covers claims arising from non-physical loss, such as financial loss –loss caused by acts of negligence, failure to fulfill a fiduciary duty, or failure of a system to perform. Where General Liability insurance covers claims of bodily injury and property damage, it typically excludes coverage for claims related to the delivery of professional services. E&O coverage will protect the policy-holding vendor from potentially catastrophic litigation caused by charges of professional negligence or failure to perform its professional duty and help to reimburse the Cloud client for claims arising from a failure to perform, failure to protect, financial loss caused by the system, and errors or omissions in the service or product.

TROUBLE INDEMNITY

Indemnity clauses are designed to provide protection and representation to parties that are unwittingly drawn into a dispute to which they have little or no connection. They provide a contractual obligation to compensate a party for a loss or to represent its interests in court. "Standard" indemnification provisions typically address liability for physical harm that may befall a claimant due to a negligent condition or poor service – protections that are over-broad and unaligned with the context of a software licensing relationship.

Indemnification in the Cloud should address trademark infringement and unauthorized use of protected intellectual property - causes of action that are more logically applicable to a Cloud relationship. A properly crafted indemnification provision in a Cloud Software License Agreement would compensate the Cloud Client for any claims that its use of the service violated any third-party intellectual property rights, such as patent, copyright or trademark, and provide for representation should that claim involve legal action. Well-crafted indemnification provisions in a Cloud Software License Agreement are narrowly drawn; provide each party with adequate notice of claims; allow for a reasonable time to respond; secure professional representation; and provide the indemnified party with sufficient control over the final outcome should it adversely affect it.

[5] "Anonymize" is a new term of art in the age of data that refers to stripping data of all its indicia of identity and mixing it with like data to set thresholds, standards, and trends that are representative of the whole data set from multiple sources, but are not traceable to any one client.

BALANCE OF EQUITIES

Connected to all of these issues is the concept of the balance of equities. Software and software relationships have changed substantially in the age of the Internet. The days of purchasing software for a large lump sum with annual maintenance costs are over. Cloud software is ubiquitous and immersive. The feature sets, functions, quality and breadth of the technology itself changes rapidly and improves over time as the vendor advances its product and applies newly available technologies. The vendor, not the client, bears the costs and obligation of maintaining the technology, including provision of redundant systems and data back-ups. License fee payments are much smaller and remain at the same level over longer periods of time. Given the heightened infrastructural demands on the Cloud vendor, the ongoing nature of the relationship, and the reduced fee structure, Cloud vendors typically require more protection than software vendors of the past and build those protections into the relationship. They are part and parcel of doing business on the Internet and, when properly balanced, protect both parties and better ensure the success of the relationship.

"Software relationships have changed substantially in the age of the Internet. The days of purchasing software for a large lump sum with annual maintenance costs are over."

▸ LIMITATION OF LIABILITY

For example, Cloud Software Licensing Agreements often include limitation of liability and limited indemnification language that provide protections concomitant with the value of the contract and the obligations imposed on the vendor. The specific nature of the liability clause and its restrictions will depend upon the type of Cloud software supplied, the value of the agreement and what is typical to the business sector in which the parties operate. Any limitation of liability clause should take the risks and rewards into account and should be reasonable to both parties. They should include reciprocity – hence the limits apply equal to both parties – and be bolstered by adequate insurance coverage.

▸ LIQUIDATED DAMAGES

Many agreements specify a fixed amount that the parties agree in advance is a fair sum to be paid for particular breach – these are known as liquidated damages and may be in the form of service credits, or lump sums. They may also include other rights like the right to terminate or to recovery of data. These forms of limitation are entirely appropriate given the changed paradigm and should be part of every Cloud Software Licensing Agreement.

IN CONCLUSION

Technology is an integral part of every business today and, therefore, every organization should have a technology-based agreement in place that addresses the unique conditions, liabilities, obligations, and challenges created by a relationship with a technology vendor. As technology changes the standards of care and underlying claims also change – as they have with the advent of Cloud software systems. To be properly protected in any vendor-client relationship, the form of the agreement must match the subject matter of the relationship.

Standard service agreements are inappropriate for modern day Cloud service relationships and likely cause more problems than they prevent. Having an approved agreement to work with may give the would-be Cloud client comfort that the legal issues are adequately addressed, but that security is as old a concept as the paper it's written on.