Key Issues and Guiding Principles for Drafting Cloud Computing Agreements

Authors: Matthew A. Karlyn, Michael R. Overly, and Christopher C. Cain

FOLEY

FOLEY & LARDNER LLP

Key Issues and Guiding Principles for Drafting Cloud Computing Agreements

This document provides an overview of many of the critical issues that arise in drafting and negotiating cloud computing agreements from the perspective of the client of the cloud computing vendor. Cloud computing can be described as “standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way” (Forrester Research) and “the provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis” (Gartner). Cloud computing has become known by several different acronyms such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Regardless of the nomenclature, cloud computing essentially involves accessing a vendor’s software and infrastructure remotely and oftentimes includes storing your data with that vendor. To that end, cloud computing agreements have some similarity to traditional software licensing agreements but often have more in common with hosting or application service provider agreements.

In a traditional software licensing engagement, the vendor installs the software in the client’s environment. The client has the ability to have the software configured to meet its particular business needs and retains control over its data. In a cloud computing environment, the software and the client’s data are hosted by the vendor, typically in a shared environment (i.e., many clients per server) and the software configuration is much more homogeneous across all clients. Accordingly, the client’s top priorities shift from configuration, implementation and acceptance to service levels (availability, responsiveness and remedies) and data (security, redundancy and use). However, like a traditional software licensing agreement, provisions such as insurance, indemnity, loss limitations and warranties remain important as well. Please note, for simplicity this document refers to “software” whenever discussing the cloud offering a vendor provides, even though a particular offering may include services, infrastructure or software or a mixture.

1. Service Levels

One of the most critical aspects in drafting and negotiating a cloud computing agreement is establishing appropriate service levels in relation to the availability and responsiveness of the software. Because the software is hosted by the vendor, outside the control of the client, service levels serve two main purposes. First, service levels assure the client that it can rely on the software in its business and provide appropriate remedies if the vendor fails to meet the agreed service levels. Second, service levels provide agreed upon benchmarks that facilitate the vendor’s continuous quality improvement process and provide incentives that encourage the vendor to be diligent in addressing issues. The most common service level issues that the client should address are: (a) uptime, (b) response time, and (c) problem resolution and remedies.

(a) Uptime Service Level

The vendor needs to provide a stable environment where the software is available to the client at least during the client’s “normal” business hours, if not 24/7. The uptime service level addresses this issue by having the vendor agree that the software will have an uptime (i.e., availability) of a certain percentage, during certain hours, measured over an agreed upon period. By way of illustration, here is an example of this type of provision:

Vendor will make the software Available continuously, as measured over the course of each calendar month period, an average of 99.99% of the time, excluding unavailability as a result of Exceptions, as defined below (the “Availability Percentage”). “Available” means the software shall be available for access and use by Client. For *purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement, and the software shall not be considered Un-Available, if any such inaccessibility is due to: (i) Client's acts or omissions; (ii) Client's Internet connectivity; and (iii) Vendor's regularly scheduled downtime (which shall occur weekly, Sundays, from 2 am – 4 am central time).*

The specific service level targets depend on the facts and circumstances in each case, including the relative leverage during negotiation. Clients should not simply accept the default vendor positions on uptime percentages, measurement periods and exceptions, but should instead negotiate terms that address the client's business needs. Moreover, a client should carefully consider the outage measurement window (e.g., daily, monthly, quarterly). Vendors tend to want longer measurement periods because they dilute the effects of a downtime and thus make remedies less available to the client. Clients should receive written documentation of a vendor's scheduled downtime and ensure the window creates no issues for the client's business. Clients may also request the vendor be pro-active in detecting downtime by explicitly requiring the vendor to constantly monitor the "heartbeat" of all its servers through automated "pinging." Requiring the vendor to do this should result in the vendor knowing very quickly that a server is down without having to wait for a notice from the client. Finally, the concept of "unavailability" should also include severe performance degradation and inoperability of any software feature – see the section below on Response Time Service Level.

(b) Response Time Service Level

Closely related to and, in fact, often intertwined with the uptime service level is the response time service level. This service level sets forth maximum latencies and response times that a client should encounter when using the software. Remote software that fails to provide timely responses to its users is effectively unavailable. As with the uptime service level, the specific service level target depends on the facts and circumstances in each case, including the complexity of the transaction at issue and the processing required. Note that response time service levels are typically included with the definition of "availability" set forth in the uptime service level section. An example provision of a response time warranty:

Vendor guarantees that __% of software transactions will exhibit __ seconds or less response time, defined as the interval from the time the user sends a transaction to the time a visual confirmation of transaction completion is received.

(c) Problem Resolution Service Level and Remedies

The vendor's obligation to resolve issues in a timely manner needs to be included in any cloud computing agreement. Vendors often include only a response time measurement, meaning the time period from when the problem is reported to when the vendor begins working to address the issue. These obligations typically fall short of what is necessary. The service level should instead include both an escalation matrix (defining both levels of severity and estimated response times for each) and specific vendor obligations to address the problem or provide an acceptable workaround.

Remedies should cover both a failure to hit a service level and a failure to timely resolve a reported support issue. Typically, these remedies start out as credits towards the next period's service. For example, a remedy might provide: for every X increment of downtime below the agreed upon level in the measurement period, or for every Severity level 1 support issue vendor does not resolve within the stipulated time, client receives 5% of next month's bill, up to a maximum credit of 75%. The remedies should scale such that if repeated failure occurs, the client should have the right to terminate the agreement without penalty or having to wait for the current term to expire. Here is a portion of a sample remedy provision for a service level failure; the provision for a support failure could be similarly drafted:

In the event the software is not Available 99.99% of the time but is Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Client shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. In the event the software is not Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Client shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. Additionally, in the event the software is not Available 99.99% for (a) three (3) months consecutively or (b) any three (3) months during a consecutive six (6) month period, then, in addition to all other remedies available to Client, Client shall be entitled to terminate this Agreement upon written notice to Vendor with no further liability, expense or obligation to Vendor.

2. Data

The vendor's use of client data and the security and confidentiality of that client data are very important in a cloud computing agreement. The vendor should provide detail regarding, and agree to reasonable provisions addressing, its competency, policies and procedures related to: (a) protection against security vulnerabilities, (b) disaster recovery and business continuity, (c) data backups, and (d) the use of, and return of, client data.

(a) Data Security

The need for data security is obvious. While it might seem that cloud computing vendors would want their agreements to include detail about their data security, they too often do not. Accordingly, clients should demand that vendors provide specific details in the agreement about data security, specifically hardware, software and security policies. These details need to be reviewed by someone competent in data security – either someone within the client's organization, a data security attorney or a third-party consultant. Some vendors will not distribute copies of their security policies but will allow clients to come to the vendor's site and inspect them. Such policy inspection should be done if the client information at issue is very sensitive or mission critical. A client should compare the vendor's policies to its own, and in fact, many clients demand the vendor match the client's policies. The client should also consider verifying the vendor's capabilities via a physical visit or SAS 70 audit (IT internal controls audit) conducted by a third party, or both. It is becoming far more expected that vendors regularly demonstrate to their clients that their security controls remain intact and robust.

Consider the following sample of a typical data security provision:

a. In General. Vendor will maintain and enforce safety and physical security procedures with respect to its access and maintenance of Client Information that are (a) at least equal to industry standards for such types of locations, (b) in accordance with reasonable Client security requirements and (c) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of Client Information and all other data owned by Client and accessible by Vendor under this Agreement.

b. Storage of Client Information. All Client Information must be stored in a physically and logically secure environment that protects it from unauthorized access, modification, theft, misuse and destruction. In addition to the general standards set forth above, Vendor will maintain an adequate level of physical security controls over its facility. Further, Vendor will maintain an adequate level of data security controls. See Exhibit A for detailed information on Vendor's security policies protections *c. Security Audits. During the Term, Client or its third party designee may, but is not obligated to, perform audits of Vendor environment, including unannounced penetration and security tests, as it relates to the receipt, maintenance, use or retention of Client Information. Any of Client's regulators shall have the same right upon request. Vendor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.*

(b) Disaster Recovery and Continuity

Disaster recovery and continuity provisions require the vendor to demonstrate and promise that it can continue to make the software available even in the event of a disaster, power outage or similarly significant event. Too often the client does not request these provisions or, even if it does, it does not read the actual vendor policies and procedures. This is foolish because the client will not have its own, up-to-date backup of the data used with the software. Without access to such data and software, the client's business may falter. Thus, the client needs contractual assurance regarding disasters and continuity. By way of illustration, here is a sample provision of what to ask of the vendor in this regard:

Vendor shall maintain and implement disaster recovery and avoidance procedures to ensure that the software is not interrupted during any disaster. Vendor shall provide Client with a copy of its current disaster recovery plan and all updates thereto during the Term. All requirements of this Agreement, including those relating to security, personnel due diligence, and training, shall apply to the Vendor disaster recovery site.

(c) Data Redundancy

Because the client relies on the vendor as the custodian of its data, the client should demand the cloud computing agreement contain explicit provisions regarding the vendor's duty to back up client data and the frequency of that back up. A good place to start is for the client to compare the vendor's backup policies to its own and make sure they are at least as stringent. Below is a sample provision addressing these obligations:

Vendor will: (i) execute (A) nightly database backups to a backup server, (B) incremental database transaction log file backups every 30 minutes to a backup server, (C) weekly backups of all hosted Client Information and the default path to a backup server, and (D) nightly incremental backups of the default path to a backup server; (ii) replicate Client's database and default path to an off-site location (i.e., other than the primary data center); and (iii) save the last 14 nightly database backups on a secure transfer server (i.e., at any given time, the last 14 nightly database backups will be on the secure transfer server) from which Client may retrieve the database backups at any time.

(d) Use of Client Information; Data Conversion and Transition

Because the vendor will have access to, and will be storing, the client's sensitive information, the agreement should contain specific language regarding the vendor's obligations to maintain the confidentiality of such information and confirming that the vendor has no right to use such information except in connection with its performance under the cloud computing agreement. Moreover, data conversion, both at the onset and termination of the cloud computing agreement must be addressed to avoid hidden costs and being "locked in" to the vendor's solution.

First, more cloud computing vendors want to analyze and use the client data that resides on their servers for their own commercial benefit, in particular the data clients create as they use the software. For example, the vendor may wish to use a client's data, aggregated along with other clients' data, to provide data analysis to industry groups or marketers. The vendor may limit its use to de-identified client data. These uses are very similar to what businesses and individuals have been dealing with while surfing the Internet while “cookies” follow where we go and what we do.

Here however, the client data in the cloud is proprietary and confidential to the client and its business. As such, the client should consider such use of any of its data very carefully and, if the agreement does not mention these sort of uses, the client should ask the vendor about its uses and add a vendor representation about which uses, if any, are permitted. Most clients should conclude that the vendor should not have any right to use the client’s data, whether in raw form, aggregated, or de-identified, beyond what is strictly necessary to provide the software. An example where commercial use might be acceptable is where the vendor provides a service that directly depends on the ancillary use of such data, such as aggregating client data to provide data trending and analysis to client and similarly situated clients within an industry.

Second, the client must address data conversion issues and return of data upon termination of the cloud computing agreement. Going into the relationship, the client should know that its data can be directly imported into the vendor’s software or that any data conversion needed will be done at vendor’s cost or at client’s cost (with client’s agreement). A client should consider conducting a test run of vendor’s mapping scheme to see how easy or complicated it will be (likewise when checking vendor’s references, ask about data migration experiences). Lastly, the client does not want to be trapped into staying with vendor because of data format issues. To that point, the agreement should include explicit obligations on the part of the vendor to return the client’s data, both in vendor’s data format and in a platform-agnostic format and thereafter destroy all of the client’s information on vendor’s servers, all upon termination of the agreement. A sample provision to illustrate this obligation:

At Client’s request, Vendor will provide a copy of Client Information to Client in an ASCII comma-delimited format on a CD-ROM or DVD-ROM. Upon expiration of this Agreement or termination of this Agreement for any reason, (i) Vendor shall (a) deliver to Client, at no cost to Client, a current copy of all of the Client Information in the form in use as of the date of such expiration or termination and (b) completely destroy or erase all other copies of the Client Information in Vendor’s or its agents’ or subcontractors’ possession in any form, including but not limited to electronic, hard copy or other memory device. At Client’s request, Vendor shall have its officers certify in writing that it has so destroyed or erased all copies of the Client Information and that it shall not make any use of the Client Information.

3. Insurance

The client should always address insurance issues in cloud computing situations, both as to the client’s own insurance policies and the vendor’s insurance. Most data privacy and security laws will hold the client liable for a security breach whether it was the client’s fault or the vendor’s fault. Thus, the client should help self-insure against IT risks, including data and privacy issues, by obtaining a cyber-liability policy.

Cyber liability insurance can protect the client against a wide range of losses. Most cyber insurance policies will cover damages arising from unauthorized access to a computer system, theft or destruction of data, hacker attacks, denial of service attacks, and malicious code. Some policies also cover privacy risks like security breaches of personal information, may apply to violations of state and federal privacy regulations, and may provide reimbursement for expenses related to the resulting legal and public relations expenses.

Requiring the vendor to carry certain types of insurance enhances the likelihood that the vendor can meet its obligations and provides direct protection for the client. The primary forms of liability insurance that a vendor should be required to carry are Technology Errors and Omissions Liability Insurance and Commercial Blanket

Bond, including Electronic & Computer Crime or Unauthorized Computer Access Insurance. These types of insurance will cover damages the client or others may suffer as a result of the vendor’s professional negligence and by intentional acts by others (vendor’s employees, hackers, etc.). It is critical that the client require the vendor have these sort of policies and not just a general liability policy. Many commercial general liability policies contain a professional services exclusion that precludes coverage for liability arising from IT services as well as other exclusions and limitations that make them largely inapplicable to IT-related risks.

4. Indemnification

The vendor should agree to defend, indemnify and hold harmless the client, its affiliates and agents from any claim where the vendor breaches its obligations in regards to the confidentiality and security of the client’s data. Any intentional breach should be fully indemnified, meaning that the client will have no “out of pocket” costs or expenses related to recovery of the data and compliance with any applicable notice provisions or other obligations required by data privacy laws. In the event the data breach is not intentional, the vendor may require a cap on its potential liability exposure, which may be reasonable depending on the type of client data in question.

The vendor should also agree to defend, indemnify and hold harmless the client and its affiliates and agents from any claim that the software infringes the intellectual property rights of any third party. This means that the client will never be “out of pocket” costs or expenses if some third party claims infringement. Vendors often try to limit the intellectual property indemnification only to infringement of copyrights. That is not acceptable, as many infringement actions arise out of patent or trade secret rights. The indemnity should extend to infringement claims of any “patent, copyright, trade secret, or other proprietary rights of a third party.” Avoid any restriction to patents “issued as of the Effective Date” of the agreement. Vendors usually also limit the indemnification to “United States” intellectual property rights, and that is generally acceptable, but the client should consider whether its use of the software will occur overseas.

5. Limitation of Liability

The vendor’s limitation of liability is very important in a cloud computing engagement because virtually all aspects of data security are controlled by the vendor. Thus, the vendor should not be allowed to use a limitation of liability clause to unduly limit its exposure. Instead, a fair limitation of liability clause must balance the vendor’s concern about unlimited damages with the client’s right to have reasonable recourse in the event of a data breach or other incident.

A vendor’s limitation of liability clause usually (i) limits any liability of vendor to the client to the amount of fees paid under the agreement or a portion of the agreement (e.g., fees paid for the portion of the software or services at issue), and (ii) excludes incidental, consequential (for example, lost revenues), exemplary, punitive and other indirect damages. While a client may not be able to eliminate the limitation of liability in its entirety, the client should ask for the following concessions:

- The limitation of liability should apply to both parties. The client should be entitled to the same protections from damages that the vendor is seeking;

- The following should be excluded from all limitations of liability and damages: (i) breach of the confidentiality provision by either party; (ii) claims for which vendor is insured; (iii) the parties’ respective third party indemnity obligations; (iv) either party’s infringement of the other party’s intellectual property rights; and (v) breach of the advertising/publicity provision (see item 9 below); and

- The overall liability cap (usually limited to fees paid) should be increased to some multiple of all fees paid (e.g., two to four times the total fees or the fees paid in the twelve months prior to the claim arising). Keep in mind that the overall liability cap should not apply to the exclusions in the bullet point above.

6. License/Access Grant and Fees

The license or access grant in a cloud computing agreement encompasses three main issues: permitted use, permitted users and fees. The grant as to permitted use should be straightforward and broadly worded to allow the client full use of the software. For example, “Vendor hereby grants Client a worldwide, non-exclusive right and license to access and use the software for Client’s business purposes.” Vendor agreements often try to limit the client’s use of the software to “its internal purposes only.” Such a restriction is likely too narrow to encompass all client’s desired uses. Drafting the license in terms of permitting the client to use the software for “its business purposes” is a better, more encompassing approach.

The license rights related to which of, and at what price, client’s constituents can use the software can be far more complicated. As to permitted users, the client must carefully define this in light of its needs and its structure. For example, beyond client’s employees, the client may want affiliates, subsidiaries (now or hereafter existing), corporate parents, third parties such as outsourcers, consultants and independent contractors all to have access to the software. The agreement should clearly set forth those users that fit the client’s anticipated needs.

As to pricing, the options are myriad. A vendor may make software available on an enterprise basis, per user, per account, per property, per X increment of use or processing power or X megabytes of storage, just to name a few. They will often charge for storage in excess of a base amount. The client’s future use of the software is also an important consideration when negotiating fees. The agreement should anticipate and provide for the ability to add or remove users (or whatever unit the metric is based on), with a corresponding adjustment of the license fees. The best time for the client to negotiate rates for additional use is prior to signing the agreement. Clients should also attempt to lock in any recurring license fees for a period of time (one to three years) and thereafter an escalator based on CPI or other third party index.

7. Term

Because the software is being provided as service, like any service, the client should be able to terminate the agreement at any time without penalty upon reasonable notice (14 to 30 days). The vendor may request a minimum commitment period from the client to recoup the vendor’s “investment” in securing client as a client (i.e., sales expenses and related costs). If the client agrees to this, the committed term should be no more than one year and the vendor should provide evidence of its up-front costs to justify such a requirement.

8. Warranties

In a cloud computing agreement, the key warranties as to uptime and access are covered by the service levels. Warranties regarding data security, redundancy and use were previously covered. Beyond those, there are other warranties that are typically included in such agreements.

The vendor should warrant the following:

- The software will perform in accordance with the vendor's documentation (and any agreed upon client-specifications);
- All services will be provided in a timely, workmanlike manner, in compliance with industry best practices;
- The vendor will provide adequate training, as needed, to client on the use of the software;
- The software will comply with all federal, state and local laws, rules and regulations;
- The client's data and information will not be shared with or disclosed in any manner to any third party by vendor without first obtaining the express written consent of client;
- The software will not infringe the intellectual property rights of any third person;
- The software will be free from viruses and other destructive programs;
- There is no pending litigation involving vendor that may impair or interfere with the client's right to use the software; and
- The vendor has sufficient authority to enter into the agreement and grant the rights provided in the agreement to the client.

9. Publicity and Use of the Client Trademarks

The client's reputation and good will are substantial and important assets. This reputation and good will are often symbolized and recognized through the client's name and other trademarks. Accordingly, every agreement should contain a provision relating to any announcements and publicity in connection with the transaction. The vendor should be prohibited from making any media releases or other public announcements relating to the agreement or otherwise using the client's name and trademarks without the client's prior written consent.

10. Notification for Security Issues

The cloud computing agreement should require that if a breach of security or confidentiality occurs, and it requires notification to client's customers or employees under any privacy law, then client should have sole control over the timing, content, and method of such notification. The agreement should also provide that if the vendor is culpable for the breach, then the vendor must reimburse client for its reasonable out-of-pocket costs in providing the notification.

11. Assignment

The client should be able to assign its rights under the agreement to its affiliates and other entities which may become successor or affiliates due to a reorganization, consolidation, divestiture and the like. Any concerns the vendor may have from an assignment can be addressed by the requirement that the assignee will accept all of the client's obligations under the agreement. Similarly, the client should also obtain assurance that any vendor assignee will agree to be bound by all of the terms and conditions of the agreement, including without limitation, service level obligations.

12. Pre-Agreement Vendor Due Diligence

Lastly, consider doing pre-agreement diligence on the vendor. By crafting and using a vendor questionnaire, the client can, at the outset, get a good idea the extent to which the vendor can meet the client's expectations and where gaps exist, eliminate them or negotiate through them. Examples of the items to cover in such a due diligence questionnaire include vendor's financial condition, insurance, existing service levels, capacity, physical and digital security, disaster recovery, business continuity, redundancy and ability to comply with applicable regulations.

In conclusion, cloud computing agreements, like traditional software license agreements, should be negotiated with the client's needs in mind as vendor forms invariably are one-sided. Unlike traditional software licenses however, the client needs to focus less on configuration of the application and more on its availability and the security of client's data.