International In-house Counsel Journal
Vol. 6, No. 23, Spring 2013, 1

Cloud Computing: Contracting and Compliance Issues for In-House Counsel

SHAHAB AHMED
Director – Legal and Corporate Affairs, Microsoft, USA

Abstract:

Many organizations across the world are adopting Cloud based services, to reduce information technology ("IT") costs and to meet rapidly growing business demands. Organizations now have to think about purchasing IT as a service, instead of making the traditional hardware and software purchase decisions. This fundamental paradigm shift is not only challenging for procurement professionals, it also presenting new challenges for the in-house counsel, who are often involved in negotiating large Cloud services agreements. Cloud services contracts are different compared to the traditional IT outsourcing agreements, since a Cloud service is designed as a multi-tenet service, where computing and operating resources are shared across potentially millions of customers – making the scale and consistency extremely important to the viability of the Cloud business model. This paper will examine recent trends and well as areas of significance in a Cloud services agreement such as Defined Terms, Service Level Agreements, Data Privacy and Security, Regulatory Compliance as well as traditional agreement aspects such Audit Rights.

Introduction:

The term "Cloud computing" has gained significant popularity recently, with many Information technology ("IT") vendors using the term to market their services. In its most classical sense, Cloud computing is the delivery of computing functionality and power to devices such as PCs, tablets, and smart phones, from remotely located data centers ("the Cloud"), using the public internet infrastructure. Many of us use the Cloud on a frequent basis when we use internet-enabled and mobile consumer services such as Facebook, Bing, Google, as well as enterprise services such as Office 365. This paper focuses on the enterprise Cloud services since in-house counsel often engage in contract negotiations for the enterprise Cloud and on the Cloud's regulatory compliance aspects.

Many in-house counsel have negotiated IT outsourcing agreements for decades, but they are relatively new to Cloud contracts. Cloud computing is a fairly new computing model, made possible by advances in computer and internet technology, and it differs significantly from traditional IT outsourcing in many respects. Naturally, some confusion exists over the differences between Cloud computing and traditional IT outsourcing, and sometimes, there is a desire to apply traditional IT outsourcing principles and negotiation tactics to the Cloud computing.

This paper explains the key differences between Cloud computing and traditional IT outsourcing arrangements, and outlines potential contractual and compliance implications that result from such differences.

Essential Characteristics of Cloud Computing:

The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as:

> *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[1]

There are many enterprise Cloud services available in the marketplace today. While each of the Cloud vendors may operate differently, there are certain commonalities that are important to discuss in order to have a good understanding of technology, business and contractual implications.

The Cloud business model is often dependent on receiving relatively small sums of revenue from a very large base of customers. Many Cloud vendors serve millions of customers from a single technology platform and operations model, making the scale and consistency a critical factor for controlling operating expenses. Since this model leverages economies of scale to deliver computing services at lower costs, Cloud vendors often have little appetite for customization. For instance, Cloud vendors often use sub-contractors for support, technical expertise, and other reasons. These sub-contractors serve the entire customer base on the Cloud platform so it not feasible for an individual customer to veto specific sub-contractors.

Another aspect of the Cloud technical architecture is the "multi-tenant" nature of the platform. The functional and technical aspects of the Cloud are designed to serve a large customer base from the same platform, limiting the opportunities for customization. Cloud economics also depends on the ability of Cloud service providers to operate large, inter-connected, efficient, and strategically placed data centers. The location of these data center depends on many factors including geographic proximity to the customers, operational cost structures, legal and regulatory environments, political and safety concerns, among others. These data centers are typically connected over a network to move the data between data centers for backup, load balancing, and disaster recovery purposes.

Essential Characteristics of Bespoke Outsourcing Arrangements:

Businesses have been entering in bespoke IT outsourcing arrangements for decades. In a typical IT outsourcing arrangement, a customer outsources all or parts of its IT functions to a traditional large IT outsourcing provider such as IBM or HP.

IT outsourcing deals are typically large multi-million or multi-billion dollar, multi-year deals. According to a recent report[2], the average value over the life of the contract of outsourcing deals is around hundred million dollars, with an average deal tenure of five and half years, with many mega deals reported in excess of one billion dollars. An outsourcing customer exercises a great deal of control over the operations of outsourcing arrangements since each contract is designed for an individual customer with specific needs in mind. While it is true that an outsourcing provider wants some control, the customized nature of the deal provides flexibility to accommodate unique functional and operational requirements, since the costs are directly passed back to the individual customer. For example, if a customer wants the databases to be located in a certain

[1] http://www.nist.gov/itl/csd/cloud-102511.cfm

[2] http://www.kpmginstitutes.com/shared-services-outsourcing-institute/insights/2012/pdf/kpmg-deal-tracker-apr-to-jun-2012.pdf

location, the IT outsourcer is usually able to accommodate such a request. The economic power of a customer in an outsourcing arrangement is also significant due to size of the deal and stakes involved.

The technology architecture of the outsourcing platform is also customized. It may include handing over existing IT systems and personnel to the outsourcer for on-going operations and maintenance. It may also include usage of the outsourcer's proprietary systems as well as the development of new systems.

The key element to understand is that unlike the Cloud services, everything about an IT outsourcing arrangement is designed to address the specific needs of the individual customer, which allows a great deal of flexibility in negotiating customized contracts.

	Cloud computing	**Bespoke IT Outsourcing Arrangement**
Business Model	• Scale – Large and diverse customer base with smaller revenue streams per transaction • Operating control is critical due to cost pressures	• Size of the Deal – Large multi-million or multi-billion dollar and multi-year deals • Individualized deal allows the flexibility to transfer costs back to individual customers
Operating Model	• Economies of scale requires consistency in processes and operations • Shared "multi-tenant" platform serves potentially millions of customers • Less flexibility to develop customized features or operating requirements	• Bespoke nature of the deal allows outsourcers to customize each arrangement • Platform built to accommodate individual customer needs with the customer directing the arrangement • Features and operations can be developed to address individual customer needs
Costs	• Shared platform and operations allows the operating costs to be distributed across large base of customers, leading to lower costs due to economies of scale	• Higher costs due to bespoke nature of the deal • Customer directly finances cost of the outsourcing arrangement

Hybrid Models:

As the Cloud computing industry evolves with customer needs, Cloud providers are creating offerings that combine characteristics of both Cloud computing and outsourcing. For instance, a Cloud provider may offer a traditional Cloud service but allow customers to purchase a "premium" support service, which includes dedicated support staff for an individual customer, as long as the customer is willing to pay the associated costs. A Cloud provider may also apply a "go regional" strategy, where its data centers are located in major markets across the globe instead of a few centralized data centers. While these hybrid models are interesting, they present similar trade-offs and contractual ramifications as those discussed in this paper.

Contract Negotiations for Cloud Services:

In-house counsel often engage in tough and adversarial contract negotiations with IT service providers. A sound understanding and knowledge of the Cloud business model helps to reduce friction in the process. In order to prepare for the negotiation process, it is important to understand the interests and the negotiating parameters of each party, in order to try to come to the most appropriate arrangement for both parties.

IT outsourcing contract negotiations may seem to provide a greater level of flexibility due to the unique nature of each deal. In-house counsel can sometimes become frustrated when the Cloud services contracting process does not appear to offer the same level of

freedom. The reason behind the different approach is not usually the unwillingness of Cloud vendor to negotiate; instead, it is the turnkey nature of the Cloud services, which leaves less room for customizing the contractual terms. In fact, in-house counsel should be vigilant when a Cloud vendor agrees to terms which run counter to their business model and operations strategy.

Most enterprise Cloud vendors offer standard contractual terms since the scale, the multi-tenant design, and the turnkey nature of the cloud demands the contracting process be fairly standard.

Defined Terms:

It is important to understand the key operative definitions since they relate directly to the operations of Cloud services. For example, a contract may define the term "financial data", and describe the handing of financial data by the Cloud provider. The defined terms in the contract often do and should reflect how the back-end systems are designed and operated. A customer may want to change contractual definitions, but this is often not possible due to the way the Cloud systems operate. Changing a definition may mean modifying the system design and operations, which can be very disruptive and cost prohibitive. Instead of focusing on changing defined terms, in-house counsel should work to understand the definitions in order to assess if the Cloud service fits their business needs.

New Feature Development:

In traditional outsourcing arrangements, individual customers exert a great deal of control over features and functionality, since the customer is directly financing the arrangement. On the other hand, a typical Cloud vendor develops and deploys features based on its assessment of the overall market demand. While there may circumstances when a large customer can influence the Cloud service roadmap, in most cases, individual customers won't be able to control the prioritization of their Cloud service provider's work. In-house counsel may be more successful requesting Cloud service providers to commit to service roadmaps, instead of negotiating specific features and functionality.

Terms and Conditions around Operations of the Cloud Services:

While there is always an interest on the part of potential customers to negotiate how aspects of services are operated, it is not likely that a Cloud vendor will change its operations to meet the unique needs of an individual customer. Instead of debating unique language in the contract, the customer should work with the Cloud vendor to make an assessment in order to determine if the Cloud operations fit its needs and understand its processes and controls. Several large Cloud vendors adhere to standards and certifications to demonstrate the capabilities of their Cloud services, and potential customers should ask for such certifications as means of verification.

Data Location Requirements:

Data location has become a hotly debated topic in the industry, with privacy advocates and regulators raising concerns about the risks of moving data to new jurisdictions. To date, there is no empirical evidence that data is safer in one geographic location compared to others. Cloud economics demands scale, which means most customers are served from geographically dispersed data centers. It also means that unless by chance the customer happens to be operating in the jurisdiction where the data center is located, the customer will probably be served from a remote data center location. Even if the customer is located in the same jurisdiction as the data center, the customer data is probably transferred to other locations for the purposes of backup and disaster recovery, redundancy, support and other technical and operational reasons. Instead of focusing the

energy on a negotiating a specific location of the data center in the negotiation process, potential customers should ask for transparency regarding where the main data sets are stored, and associated data flows to make sure their needs are being addressed.

European Union Data Transfer Requirements:

The European Union has specific rules around transfer of personal data outside the European Economic Area. Since many large Cloud vendors are based in United States, there is often a need to transfer data to United States, for a variety of reasons. Many reputable Cloud vendors have achieved the certification under the U.S.-EU Safe Harbor Framework, which allows them to transfer data to the United States under EU rules. It is important for customers to check for the certification status of their Cloud vendors on the U.S. Department of Commerce web site.[3] While the U.S.-EU Safe Harbor Framework is a legitimate way to transfer data, a few privacy regulators have called for more robust mechanisms and controls.

Cloud vendors, which are focused on satisfying the data protection needs of enterprise customers, may also offer the EU's Standard Contractual Clauses.[4] The Standard Contractual Clauses, which are published by the European Commission, are a robust and legally valid way to transfer personal data outside of the EEA.

In-house counsel should push for clarity on legal mechanisms that are being used by Cloud vendors to transfer data outside Europe to ensure compliance with EU rules. If the client has specific data protection concerns, in-house counsel should seek to incorporate the Standard Contractual Clauses in the contract framework, as a way to provide additional assurance that data can legally flow to the Cloud.

Data Privacy and Security Requirements:

The privacy and security of personal data has become a top area of concern in the Cloud computing industry due to concerns about how customer data may be mined (for example, to provide targeted advertising). Customers are legitimately concerned about the privacy and security practices of Cloud vendors.

In-house counsel should demand a detailed data processing agreement from Cloud vendors to ensure privacy, security, and confidentiality terms are properly addressed and meet the needs of the customer. In-house counsel should seek clear terms in their data processing agreements about how their Cloud providers will use customer data and ensure the use of that data is limited to providing the cloud services to the customer. For example, the cloud vendor should not be able to mine or use data for other purposes, such as to support consumer services like advertising.

Applicable Law and Jurisdiction:

Typical outsourcing agreements are executed in a particular jurisdiction with defined applicable law provisions, negotiated between the contracting parties in accordance with the unique nature of each deal. On the other hand, Cloud vendors usually decide on a few jurisdictions across the world as operating bases. For instance, a multi-national Cloud provider may choose Ireland as a base to operate its operations across Europe, and as a result use an Irish entity to execute contracts with standard terms defining the applicable jurisdiction and governing laws.

While some potential customers may have concerns about this approach, this is the prevalent practice among major Cloud vendors in order to sustain a scalable global business. The Standard Contractual Clauses provide greater level of flexibility to

[3] https://safeharbor.export.gov/list.aspx
[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_en.pdf

establish applicable laws. In-house counsel, who want greater flexibility in this area, should strongly consider Standard Contractual Clauses to make sure their unique requirements are being met.

Examination and Audit Rights:

In a typical outsourcing arrangement, the customer may exert control by negotiating examination or audit rights to assure appropriate documentation and compliant operations. It is very difficult for a Cloud vendor to provide such rights since the Cloud vendor could not possibly have a millions of customers examining its data centers or other operations. Direct customer audits would not only be cost prohibitive, they would also be extremely disruptive to the operations, potentially putting at risk the data and operations of other customers whose data is processed at the same location. Maintaining security is a key reason why cloud vendors generally avoid granting customers access to data centers.

Cloud vendors that sell to enterprise customers have recognized this challenge and provide independent third parties audit summary results and certifications, such as ISO 27001, as way to meet the customer needs. This approach satisfies the need for the customers to have assurance that the Cloud vendor is compliant, and it is also less disruptive to the Cloud business. Potential customers should ask for and negotiate terms which focus on independent verification by reputable third party auditors instead of focusing on direct audit rights.

Service Level Agreements:

For Cloud services, detailed service level agreements (SLAs) are usually considered an appropriate way to define the expectations around service operations and up-times. Large Cloud vendors provide written SLAs backed by financial ramifications. Potential customers should ask for detailed SLAs as well as appropriate financial terms to ensure that the Cloud vendor is strongly motivated to meet the SLAs.

Indemnification:

While a detailed discussion on intellectual property issues is outside the scope of this paper, it important to recognize that copyright, patent or trademark infringement claims by third parties is always a possibility when dealing with technology solutions. Customers should ask for terms that provide them relief on third party claims that may arise from the products and services made available by the Cloud vendor.

Regulatory Compliance:

The regulatory compliance aspects of Cloud services have been a topic of hot debate across the world. Large and reputable Cloud vendors perform rigorous analyses to make sure they are compliant with generally applicable laws. For instance, in European Union, many Cloud vendors may qualify as data processors since they process personal data on behalf of the customer, in the meaning of the EU's 1995 Data Protection Directive, and must comply with the applicable provisions of that directive. It is important to understand however, that the customer itself is ultimately responsible for compliance with laws and regulations. In-house counsel should seek guidance from their own compliance departments to ensure they are aware of the compliance requirements.

There are also many sectorial regulations that are applicable to companies in particular industries such as banking, education, and healthcare, among others. For instance, the Gramm-Leach-Bliley Act ("GLBA") applies to many financial services firms in United States. These regulations do not generally apply directly to Cloud vendors. However, Cloud vendors should provide detailed information to potential customers about how the Cloud can help customers comply with such requirements. In-house counsel should ask

for detailed written commitments from the Cloud vendors, such as in data processing agreements, to help understand how the underlying Cloud services and its operations can contribute to the customer's compliance strategy.

Many healthcare industry participants in the United States must comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), which among other things, require covered entities protect the privacy and security of protected health information. U.S. healthcare customers should obtain commitments from Cloud vendors that process protected health information that meet the "business associate agreement" requirements established by the U.S. Department of Health and Human Services.

Along similar lines, the Family Educational Rights and Privacy Act of 1974 ("FERPA") is applicable to many educational entities that receive federal funding in the United States. Among other things, it is important for such entities to comply with certain privacy provisions. Education sector customers should carefully review the requirements under FERPA ensuring that the Cloud vendor is providing adequate contractual assurances, including express commitments that data will not be mined by the Cloud vendor for purposes of advertising.

	Cloud Computing	**Bespoke IT Outsourcing Arrangement**
Defined Terms	• Lower level of flexibility to change the Defined Terms since they relate to the backend systems and processes used by the platform	• Bespoke nature of the deal allows for more control over the Defined Terms
New Feature Prioritization	• Lower costs per feature due to economies of scale, along with lower level of control over the feature prioritization	• More control to prioritize features since the customer is directly bearing the costs
T&Cs on Cloud Operations	• Scale and Consistency of the Cloud requires that the T&Cs across customers remain consistent	• Bespoke deal provides more control over operations since customer is directly paying the costs
Data Location	• Large and regionalized data centers mean lesser control over the location of the data	• Bespoke deal can call for specific location of the data and customer pays for any incremental costs
EU Data Transfer Rules	• Large and established Cloud vendors provide the EU Standard Contractual Clauses	• The Customer can negotiate unique data transfer arrangements since the costs are passed back to the customer
Data Privacy and Security Requirements	• Large and established Cloud vendors provide world class privacy and security commitments – including adherence to ISO27001	• Data Privacy and Security commitments have be to negotiated based on customer needs and appetite for compliance related costs
	• Customers should negotiate commitments around "no data mining for advertising purposes"	
Applicable Laws and Jurisdiction	• Cloud vendors maintain consistency by operating from regional centers • Established Cloud vendors provide more flexibility through the use of the EU Standard Contractual Clauses	• Individual nature of the deal provides more flexibility to establish terms
Examination and Audit Rights	• Established Cloud vendors provide independent third party audit reports	• Direct examination and audit rights are inherent part of the overall deal
Regulatory Compliance	• Established Cloud vendors enable customers to comply with regulations such as HIPAA and FERPA	• The customer negotiates regulatory compliance requirements and directly bears the costs

Data Portability:

Cloud services can hold key customer data, and in case of termination of the agreement, it is important that the customer can take their data back. While there will be costs associated with such switch overs, customers should negotiate the terms that allows data migration as needed. In-house counsel should negotiate written commitments that the Cloud vendor does not acquire any ownership rights in the customer data. It is also important to ensure that the Cloud vendor permanently deletes the customer data, at the request of the customer, within a reasonable amount of time, to remediate any confidentiality concerns.

It is important to understand the differences between Cloud services and traditional IT outsourcing models to providing counseling to the clients and to negotiate successful deals. Cloud vendors with experience of selling to enterprise customers understand the complex needs of the commercial customers and design appropriate technologies, processes and contractual safeguards to meet such needs.

***

Shahab Ahmed in his role as a Director – Legal and Corporate Affairs, Microsoft Corporation, focuses on global regulatory and commercial issues such as Data Protection, Privacy, Security, Interoperability, Standards and other ICT regulatory frameworks. Prior to this role, Mr. Ahmed was a Director in Antitrust and Interoperability group at Microsoft where he worked on competition policy. Mr. Ahmed has held a variety of Legal, business and technical leadership roles at Microsoft since 2005. Before joining Microsoft, he held leadership roles at Fortune 500 organizations including IBM, PricewaterhouseCoopers, Target Corporation and United Healthcare Group.

Mr. Ahmed has a Bachelor's degree in Information Technology, a MBA in strategic Management and a JD degree. He has also done post doctorate technology policy work at Harvard University and holds a Certified Information Privacy Professional (CIPP) designation.