ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Moving to the Cloud? Know the Basics Before Contracting

Technology, Privacy, and eCommerce

Cheat Sheet

- **It’s the future.** In-house counsel need to understand the basics of cloud computing to be effective in the modern business environment.
- **But challenges remain.** Cloud computing comes with its own set of risks.
- **Cloud deployment models.** There are four models, which offer different value proposition and associated costs.
- **Stay informed.** In this rapidly changing space, in-house counsel should stay up-to-date on cloud developments.

Cloud computing is one of the most significant IT developments in the last three decades. It is best considered as a novel business model that decouples computing and networking resources from geographic and organizational limitations.

Put simply, cloud computing delivers software and/or other IT resources to users through a network. This model deals with computation, software, data access, and storage services, but does not require the user’s knowledge of the configuration requirements or the physical location of the servers. A Cloud Service Provider (CSP) hosts the servers and maintains the software, while the customer accesses the software through the internet (usually through a subscription).

Benefits and challenges of the cloud

Increasingly competitive markets demand substantial return on investments; it does not make much economic sense for every business to invest in underused IT resources. Opting to “move to the cloud” satisfies IT requirements and frees up capital for investment elsewhere.

The CSP’s pay-only-for-what-you-use pricing model allows users to scale up or down with the vagaries of the daily, weekly, monthly, or quarterly business cycle. Such scalability increases the appeal and makes it attractive to many businesses and individuals. Before the invention of the cloud computing model, organizations had to invest in the infrastructure, whereas now, they only need hardware (e.g., a laptop, mobile, tv, etc.) and a wifi connection; there is no need to independently acquire, install, or maintain the various elements of IT architecture.

A CSP relieves clients of IT maintenance, addressing updates, patches, and hardware or infrastructure issues. This inevitably yields additional savings for clients while increasing productivity with the transparent adoption of new and more capable applications.

But cloud technologies pose novel challenges. Consider the following when adopting a cloud model:

- **Compliance.** There may be data localization restrictions, cloud computing security requirements, data privacy laws, payment card industry requirements, and financial reporting laws in each jurisdiction.
- **Commingled data.** In a cloud setting, the customers’ data gets commingled with other users’ data. Most CSPs will have secure, scalable, and customizable multi-tenant applications. However, customers should always be curious about security and privacy issues. Depending on the circumstances, they may want to consider investing in data encryption to support data confidentiality.
- **Cloud security policy/transparency.** CSPs must have proper information security policies in place and must make them transparent to the customers to avoid conflicts with the customer’s information compliance needs. The customers should demand detailed service level agreements (SLAs), which will set out the level of security provided by the CSPs.
- **Transfer and migration of data.** Before the services have started, the customers should analyze whether the CSP uses an interface, which can prevent the transfer and migration of data to another CSP.
- **Disaster recovery**. Every CSP should have a robust disaster recovery plan and customers should seek to analyze such plans. The users must understand that in case of a disaster, data retrieval may become a very complicated ordeal. Once the customer starts to use the system, data may be commingled and distributed to different servers, which means that some data may be unavailable, lost, or unidentifiable.

Essential characteristics of the cloud

Cloud computing model is defined by five essential characteristics:

1. **On-demand self-service.** Users must be able to use the services without the involvement of the CSPs (automatically and unilaterally).
2. **Broad network access.** Access must be provided through networks or common platforms.
3. **Resource pooling.** A cloud environment must pool computing resources (the cloud will serve multiple customers at the same time with different physical and virtual resources. This is referred to as the multi-tenant feature of the cloud). Multiple tenants can use the same applications, share architecture and while maintaining the separation between each other.

4. **Rapid elasticity.** Based on the customer's demand, cloud systems should allow for the instant increase or decrease of resources.
5. **Measured service.** Cloud systems should have automated control and resource optimization features. These systems should be able to spread their workloads across multiple servers.

There are three important categories of cloud services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The difference between them is the level of control that each user can exert over the cloud stack.

Categories of cloud services

IaaS – Infrastructure as a Service

The CSP offers the fundamental computing resources as a service (i.e., the hardware and very basic software).

Characteristics

- The CSP manages and controls the underlying cloud infrastructure (e.g., servers, storage, network, and data centers).
- The customers can deploy any application software or operating system they wish. The customers can also have limited control over select networking components.

IaaS allows customers to minimize investment on fixed IT assets and deploy new applications and agile technologies. The IaaS paradigm facilitates widespread adoption of increasingly advanced technologies through cost sharing; each customer benefits from the investment of every other in mitigating the risk and impact of obsolescence.

Typical examples of IaaS on the market today are Amazon Web Services (AWS) and Microsoft Azure.

PaaS – Platform as a service

Like IaaS, PaaS offers cloud infrastructure (servers, storage, and network), plus the operating system.

Characteristics

- As with IaaS, the PaaS CSP manages and controls the underlying cloud infrastructure.
- The customer installs or creates the applications they want to use.
- The customer manages the applications and services that it develops, while the CSP manages everything else.

SaaS – Software as a Service

Here the CSP brings a full-fledged application (an application is an individual piece of software), on

top of an operating system, which is ready to use by the customer. The CSP installs and maintains applications on its servers, permitting customers access via the internet. The only thing the customer needs to do is to configure the application and use it in his everyday business.

Characteristics

- Consumers do not manage or control the underlying cloud infrastructure.
- CSP retains control of networks, servers, operating systems, and storage.

Cloud deployment models

There are four deployment models: public clouds, private clouds, community clouds, and hybrid clouds. Each model serves a different purpose for the customers, and they each come with a different value proposition and associated costs.

Public cloud

Public cloud services are provided by one CSP, but they can be used by the public or a large group. This deployment model is available to every paying customer.

Examples of public cloud today would be AWS or Microsoft Azure.

Community cloud

Here the infrastructure is shared between several organizations with similar interests. The management can be handled by one or more of the organizations or even a third party. This deployment model is available to a predefined group of customers.

Private cloud

Private cloud infrastructure is exclusively organized, managed, and operated by one organization and only for the purposes of that particular organization.

Hybrid cloud

This model allows for the combination of two or more distinct cloud infrastructures.

Most of the time, the decision of which deployment model to choose will be based on the costs.

Cloud service agreements

CSPs' relationship with their customers will be defined by their contract terms, most often affording customers little negotiating power. The market power of CSPs gives them oversized influence vis-à-vis the masses of potential clients. Ordinarily, these contracts will be "click-through" agreements, which will not be negotiable. However, high value customers will be able to negotiate the offending terms through a separate "addendum."

New customers may confuse cloud computing agreements with intellectual property license agreements. Cloud computing services do not offer tangible copies of software to the customers, nor

can the customers install local copies, either of which would require licensing. A cloud user receives only remote access to the software or infrastructure.

Cloud service agreements generally take one of several forms, typically a rental agreement or a service agreement. They are sometimes called Cloud Hosting Agreements, Cloud Computing Service Agreements, or Service Level Agreements. Regardless of the label, the provision of services principally by machines eliminates the need for professional services agreements (i.e., the provision of services by labor).

The variously named agreements capture most, if not all, of the qualities of subscription services.

Data management and information security

These clauses address the issues relating to data being processed by the computers. For information handled by people, you would need confidentiality clauses.

Before negotiating these clauses, in-house counsel should know what type of data will be processed and stored in the cloud, its location, and any laws that may be applicable to the data leakage or loss. If the servers are in another country, the legal counsel may want to reach out to a local attorney. The burden of the regulatory compliance should be placed on the CSP.

These clauses usually seek to define what is considered as the customer's data. Customer's data usually consists of the information provided by the customer, which will be processed or stored on computers, and the information deriving from them. These clauses address the customer's right to access, copy, erase, or modify the data.

Most contracts, where the CSP is required to collect the customer's data, will set out how long the data will be stored, and when it will be erased. The CSP will agree to use the data only for the purposes of the contract and not to disclose it to any third parties. The ownership of the data will always remain with the customer. The CSP will also promise not to move the data to another location without the customer's consent. Some CSPs include an approved regions list to their contracts where the data may be sent.

In addition, most countries have laws that impose data security standards on companies that handle personal data. Cloud service agreements may contain a clause that states that the CSP will abide by these laws. If the CSP breaches these laws, it may be fined by the government in addition to being liable toward the customer for breach of contract. The CSPs usually do not make this promise, instead, they will promise to use reasonable efforts to comply with the laws. In this case, the CSP would still be liable under the law, but not for breach of contract.

And in some contracts, the CSP will demand that the customer indemnifies the CSP against damages it may suffer because of a breach of law due to the data content. Customers will be asked to defend and indemnify the CSP for any claims by the customer's end users. This is because the CSP makes the system available to the customer but does not really have a way of calculating what the risk would be in case of data leakage (for example if the customer uploads sensitive data belonging to minor children).

It may be argued that if the CSP is at fault at leaking the data, the indemnity clauses in favor of the CSP may not be enforceable, as the courts are not likely to let the CSP benefit from their own negligence. To avoid this scenario, CSPs should specify that the customer will indemnify them if the breach was not caused by the CSP.

Most data breaches occur in three different ways

1. Outside attacks by hackers or hostile commercial or governmental organizations;
2. Intentional employee misconduct; or
3. Human error.

Adequate representations, warranties, and covenants along with indemnities should be included in a contract to cover foreseeable scenarios. The CSP should be required to notify the customers upon any suspected or actual data breach, along with the necessary remedial measures.

Conclusion

In order to avoid future risk and embarrassment, legal counsel must be aware of the data protection laws and data transfer restrictions applicable both in their own jurisdictions, and where the data will be stored or processed.

In addition, legal counsel should always try to understand the details of each transaction; the nature of the services being provided; and the data being collected, stored, processed, or transferred. The type of contract template will change depending on the nature of the data and the services.

For example, it would not make sense to insist on using a personal data processing agreement template if the data being collected is merely machine data and does not include any personal data. Also, if the transaction involves the licensing of software, as opposed to a service being provided on the cloud, it would be more appropriate to sign a software license agreement, as opposed to a service level agreement.

As we learned in law school, we shouldn't make assumptions based on incomplete information. We must examine the details of each transaction, and not refrain from asking the relevant questions until we have all the answers. That way, we can assist our internal stakeholders in a meaningful way.

To fully prepare for your switch to the cloud, learn these 15 terms you'll find in cloud service agreements.

Laura Reynaud

Senior Legal Counsel

Siemens

Laura Reynaud is senior legal counsel at Siemens. She is a US-qualified corporate and commercial lawyer with 13 years of experience in the Middle East. Reynaud specializes in commercial contracts, mainly technology contracts, IP, cybersecurity, cloud computing, and data protection. Reynaud holds an LLM focused in International Corporate and Commercial Law from King's College London. She is based in Saudi Arabia.