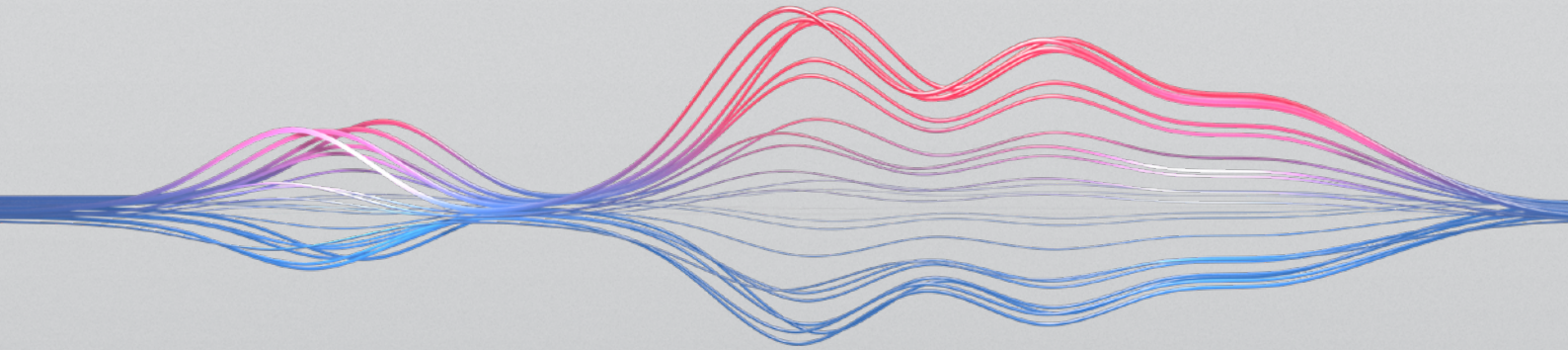
Enterprise Cloud

DISRUPTION AND RETHINKING THE STANDARD CONTRACTING MODEL



DLA PIPER

Embracing disruption in the market

In 2010 Steve Jobs predicted that the "*center of our universe is moving from PC to cloud*"[1], and he has been proved right. Users of all sizes are increasingly moving to cloud based offerings, even customers operating in the most risk adverse sectors.

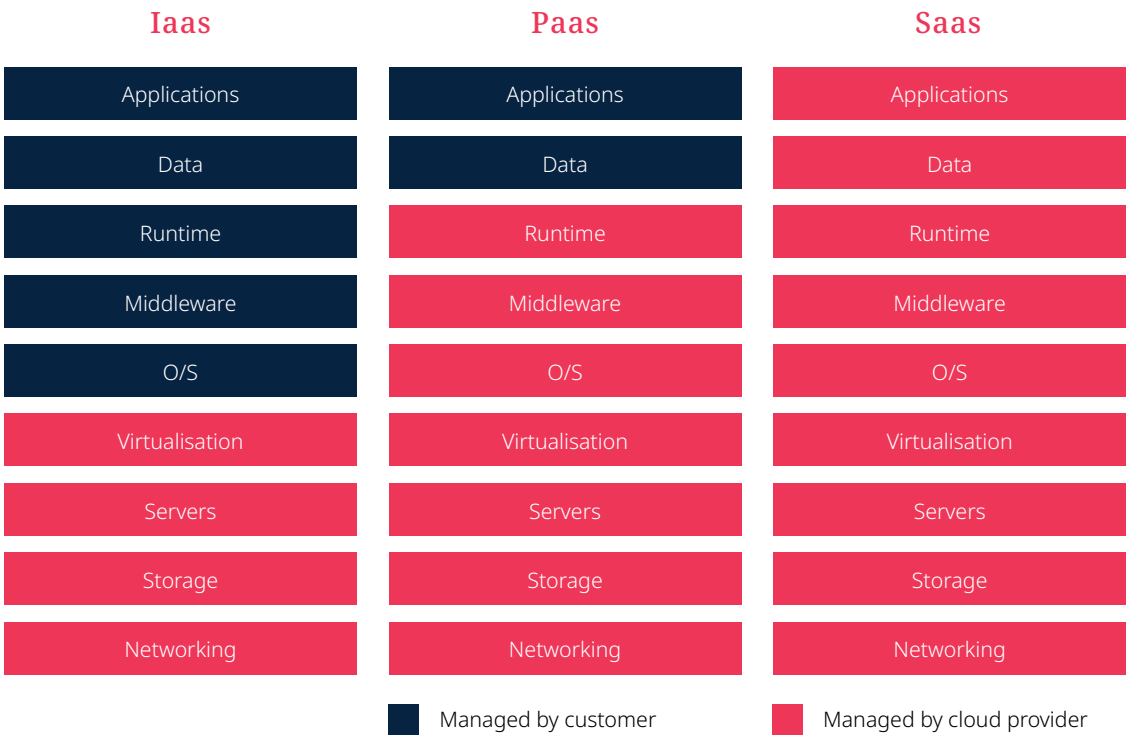
Cloud services certainly have been seen as a viable alternative to the more traditional IT solutions that typically bring with them significant investment and operating costs coupled with a lack of flexibility and scalability. Cloud-based solutions, by comparison, are commonly likened to the purchase of a utility; the cloud customer is able to purchase technology "as a service" as and when required, paying only for what it uses.

This shift in the delivery model has had inevitable consequences for technology contracting, forcing the market to look at the typical outsourcing contract in a different way. An enterprise cloud offering (whereby customers pool their enterprise-wide spend with large vendors to contract across the enterprise and benefit from economies of scale) is often supported by an agreement structured as a lean set of terms and conditions complemented by various sets of online-based terms containing evolving service levels, service descriptions and product terms. The fact that terms are offered on a uniform basis combined with the fact that the lower value of some "as a service" deals does not, ostensibly at least, justify significant legal spend and has forced customers to adopt a different approach to contracting – one where whole-sale negotiations and the traditional risk transfer might not be achievable or even appropriate. This challenge can be met by focusing discussions around key themes in order to ensure adequate customer protections.

In this paper we explore the key contractual themes when seeking to deploy an enterprise cloud solution, and suggest some approaches to managing the associated risk. First, however, it is helpful to have a basic understanding of the technology and the most common models for offering cloud solutions, as set out in Figure 1.

1 Email from Steve Jobs dated 24 October 2010

Figure 1: The cloud



In a nutshell, cloud computing offers convenient, on demand, network access to a shared pool of configurable resources (such as services, storage, applications and services) which can be rapidly released with minimal effort.[2] Broadly speaking there are three types of cloud-based models used by customers on the market:

1. **Public cloud:** services and infrastructure are held off-site by a third-party service provider, shared across their client base and accessed via public networks such as the internet. This environment allows the customer to take the benefit of economies of scale.

2. **Private cloud:** services and infrastructure are stored and maintained on a private network which can be accessed only by one customer, providing greater levels of security and control. This is also known as a dedicated cloud environment.

3. **Hybrid cloud:** combines both the public and private clouds, allowing the business customer to use the public cloud for its non-sensitive operations and a private cloud for more confidential operations.

Three principal service offerings are based on cloud technology:

1. **Infrastructure as a Service or "IaaS"** provides basic computing infrastructure such as servers, storage and networking resources. The customer can run whatever operating systems, applications and tools that it prefers on this infrastructure.

2. **Platform as a Service or "PaaS"** provides a platform allowing a customer to develop, run, and manage applications without the requirement to manage its own infrastructure which would ordinarily be associated with developing and launching an application.

3. **Software as a Service or "SaaS"** provides cloud-based applications such as office-based tools and customer relationship management software. Under this model all software and hardware is provided and managed by the cloud vendor.

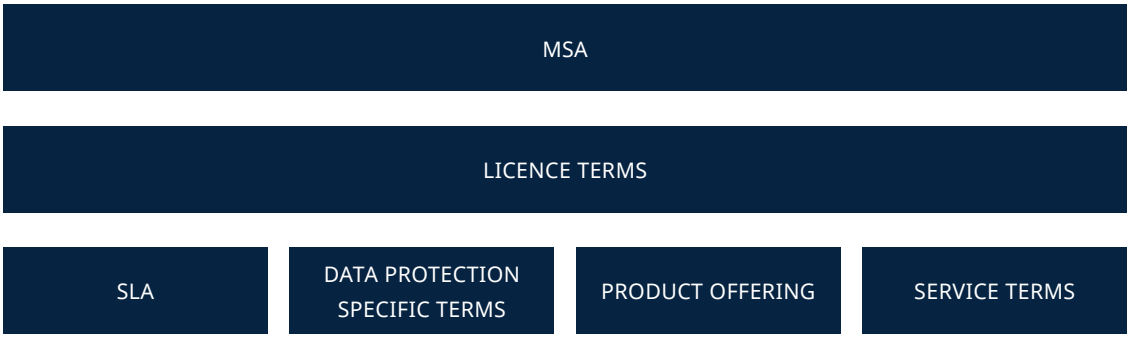
2 US National Institute of Standard and Technology.

Contracting for cloud

The different types of cloud and predominant service offerings set out in Figure 1 give rise to different risks and, accordingly, different contractual issues. Yet customers are often presented with the same contract for all scenarios. As a first step, therefore, it is essential that a customer understands the technology being used to provide the services that it wishes to procure and the extent to which the supplier is utilising a private, public or hybrid cloud to provide them. For example, we frequently see customers benefiting from a hybrid cloud model to balance the economic benefits of standard "one-to-many" services (provided from the public cloud) against the risk and regulatory requirements associated with certain datasets, for example those including personal data or particularly sensitive data (which can, perhaps, be accommodated within a customised private cloud).

The "model" form of cloud agreement issued by a supplier usually takes the form of a top level set of terms and conditions (covering key issues such as liabilities, termination rights and warranties), with accompanying documents detailing service descriptions, acceptable use policy, product terms and service level agreements. These are often presented as standard terms and conditions modelled as a one-to-many offering and put forward on the understanding that they will be subject to unilateral updates on the part of the supplier, from time to time (a point which we consider below).

Figure 2: Enterprise cloud agreement structure



This approach can make the overall agreement difficult to navigate; with embedded links and varying orders of precedence it is not difficult to "miss" a key document (particularly where parts of the contract are incorporated into the overall agreement by reference only). Constructing a diagram like the one above can be a helpful guide to tracking the main documents and ensuring that aspects which need to be amended are identified and captured in any negotiations.

That said, cloud vendors are typically averse to amending their standard contracts, arguing that it is challenging to have different contract terms for a range of clients that are, essentially, using the "same" service under the same delivery model. Deal size and nature can generate leverage and an opportunity to amend terms on the part of a customer. Moreover, the standard "one to many" argument loses some strength where the technological solution involves a private, or even hybrid, cloud – both of which remove the "one to many" characteristic.

Key issues to consider

1. Non-fixed terms

An unusual characteristic of most enterprise cloud contracts is their fluidity - the evolving and changing nature of certain aspects of the overall agreement. Whilst the principal terms and conditions will usually remain fixed, the detail of service offerings, product terms and service levels are often subject to change, being adjusted and changed at the supplier's discretion to reflect technology advances or even changes to the supplier's delivery model.

Of course, this flexibility is part of the appeal for customers as they can quickly and easily take advantage of new services and new technology. However, such changeability inevitably introduces a level of uncertainty into a contract that may well have been subject to the customer's internal risk assessment and approval process, the signed terms soon becoming superseded by the updated version. Sometimes this ability of the supplier to change terms presents more than just an internal risk issue – it can bring with it a compliance risk for the customer. For example, the customer may be subject to a regulatory requirement to control sub-contracting/ sub-outsourcing. One way for the customer to mitigate this risk is to include clear advance notification regimes around changes, agreeing longer lead times than are usually offered under the vendor's standard terms and with options for the customer in the event that the vendor's planned changes are detrimental to the customer. Similarly, the customer may negotiate the right to terminate where the changes will have a material adverse impact on its operation. The challenge, of course, is that such unplanned termination could then generate practical challenges for the customer: is this a realistic option? How easily could the customer transfer its data to another vendor and/or substitute an alternative vendor's services? The customer will need to address its "Plan B" as part of entering into the contract so that these rights are meaningful.

2. Limited contractual assurances

Another key factor for customers is that an enterprise cloud contract is unlikely to transfer as much risk to the supplier as is the case under traditional outsourcing models. As a result, customers need to take a more holistic view of how to deal with the risks involved in cloud technologies. In particular, customers should pay more attention than perhaps has previously been the case to the mitigation of risks on 'their side of the fence'; for example, in relation to operational methods around encryption of data and access rights, cyber security insurance and strong governance regimes.

Similarly, cloud providers will typically offer only limited warranties with regard to the performance of the service. This can make it difficult for a customer to bring a claim for loss resulting from the supplier's default because it may be challenging to link that loss to breach of a specific contract term. To compensate for this the customer needs to place greater emphasis on due diligence to ensure that it is comfortable that the service will be robust enough and meet its requirements, including availability, taking less comfort from contractual remedies.

3. Service offering

As mentioned above, cloud vendors base their operating model on delivering the same service to all customers (particularly for SaaS) even though the environment through which the service is deployed may differ: the "one to many" approach. We have touched upon the fluidity of contract terms. As regards the services themselves, given the dynamism of the cloud offering, customers should re-think the historic norm of lengthy service descriptions with fixed scope and instead embrace short form descriptions of cloud services which will change over the lifetime of the contract.

Turning to the contract again, customers should check whether or not the applicable terms and conditions depend upon the number, or combination, of services taken up. We often see customers consider additional support services that are being offered by cloud vendors at extra cost. In our experience, purchasing additional services tends to 'unlock' offerings in the contractual terms which can be beneficial to the customer (e.g. longer advance notification of changes).

Commercials – minimum buys and commitments

An extremely important key to unlocking more robust contractual protection is commercial leverage. The value or unique nature of a deal, or the appeal of moving to a new customer market segment, can have significant impact on the risk appetite of cloud vendors. Customers should assess the relative value of their deal over and above its face value and consider whether this can perhaps drive some flexibility on the terms.

Similarly, taking the opportunity to maximise the benefit of economies of scale by contracting on an enterprise basis, pooling buying spend across the customer's organisation where possible to do so, can result in a 'better' deal for a 'bigger' deal.

The most compelling factor relates to any minimum commitment on the part of customers. These are obviously beneficial to suppliers and can give customers some ability to argue for preferential terms. Clearly the customer needs to weigh up the benefit of any enhanced terms against the consequences of not meeting any minimum spends and commitments, especially if the customer risks being prevented from reaching the minimum buy/usage for a reason outside of its control.

4. Security and data protection

Many cloud vendors model their security and data protection related terms on the basis of a shared responsibility model which demarcates where the customer's responsibility for the cloud environment ends and where the cloud vendor's responsibility begins. This approach places a much greater emphasis on the customer's data management responsibilities than is the case under the traditional outsourcing model. The shared responsibility model has nuances dependent upon whether the service is IaaS, PaaS or SaaS, but one area which should always remain the cloud vendor's responsibility is the physical security of the data centre or location where the data and platform will be hosted.

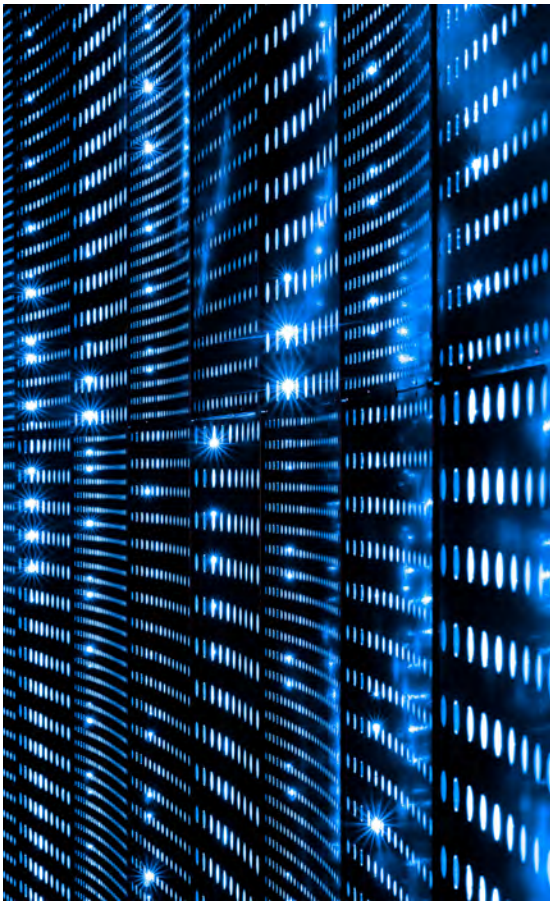
This model does, however, reinforce the perspective that enterprise cloud contracts cannot be used as a vehicle to wholly transfer security risk. It is crucial for organisations looking to move to the cloud to engage with their internal security and operational teams early on in the procurement process to ensure that adequate security controls can be put in place, such as end-to-end encryption of data, for those areas where the customer retains responsibility. The customer could, for example, retain responsibility for identity and access management and client end point protection.

The regulatory requirements where personal data is concerned are, of course, significant. Where personal data is, or may be, included in the dataset customers should assess the related terms offered by cloud vendors in light of the General Data Protection Regulation ("GDPR") or relevant local law equivalent. For GDPR compliance this will include understanding where data will be held (will it be within the European Economic Area?). As GDPR compliance applies to all (in-scope) technology contracts, in theory this aspect of the contract review does not differ significantly from non-cloud solutions. However, the challenges in practice are twofold, first, imposition of the full range of GDPR requirements on cloud vendors can be difficult. Secondly, geographically restricting the location of data runs somewhat counter to the "pure" cloud model. It can be possible to obtain commitments if not for specific data centres, at least for the geography in which the data centre is located; in fact some of the larger suppliers have now developed standard GDPR compliant offerings.

5. Sector regulatory compliance

Of particular concern for many customers is the need to address sector regulatory compliance. From a customer perspective, these are mandatory but they can be problematic as they purport to afford the customer rights which the supplier feels it cannot deliver. In the same way that some vendors offer GDPR compliance solutions, certain cloud vendors offer industry-specific contracts which offer enhanced terms to help customers meet regulatory requirements. This is particularly the case for those customers in the financial services or insurance sector which are subject to specific outsourcing and cloud requirements.

The more challenging regulatory requirements include wider-ranging audit rights and controls over sub-sourcing. Regulatory compliance is not always as simple as including specific, mandatory terms word for word. Rather, regulators are interested in identifying and managing risk in reality. This means that a degree of judgement is required in understanding how the relevant regulator might view the proposed cloud deal (e.g. is the function "critical or important"? If so, the more definitive regime applies), the application of proportionality (a fundamental concept to the application of European regulations in this area) and the risk appetite of the customer in question.



6. Exit/Termination

Termination rights will, naturally, be a key area to focus on. Sometimes the customer will need to negotiate additional rights of termination required by its regulator because the standard termination rights offered by cloud vendors are, usually, limited in scope. To an extent, the risk of contractual termination shortcomings is mitigated by the fact that many cloud commercial models are consumption based; as such, if a customer is not satisfied with a service they can simply stop using it. However, this reassurance should be considered in the context of any minimum spend commitments (or the commitments should be negotiated to be adjusted in the event of service diminution), the business interruption impact this would have and whether or not any of the regulatory contract termination requirements mentioned above apply.

Looking at the supplier's opportunity to withdraw the services, again a key area to review is its right to suspend or terminate the service, for example, is the termination being triggered on the basis of impact on the infrastructure or other emergency scenarios.

Usually, cloud exit assistance obligations are limited. Customers should not expect the lengthy exit management schedules that are traditionally included in outsourcing contracts. Instead they should focus on customer rights to access and extract data from the cloud environment following termination (often this is made available only for a limited period of time) while at the same time, considering internal plans and approach to service transition. Such planning may, again, be expected by the customer's regulator.

7. Governance

Enterprise cloud contracts are unlikely to include "heavy" service incentive regimes (such as high service credits or step in rights) unless they are significant deals supported by bespoke, negotiated, terms. Instead, the governance regime tends to takes on an enhanced significance with the aim of enabling escalation, discussion and resolution of any issues that may arise. With limited service warranties, focus will need to be applied to making sure the customer reviews and understands service performance metrics including those outside of the physical contract itself.

Embracing the disruption

Use of cloud-based technology solutions looks likely to only increase given the benefits of reliability, flexibility and cost efficiency. To take advantage of this, customers should be prepared for the enterprise cloud journey to come. This includes understanding the new way of contracting, the evolution in customers' approach managing the risks more widely, and any regulatory requirements.

Contact

For further detail or if you would like to discuss any of the issues raised here, please contact your usual DLA Piper contact or email outsourcing@dlapiper.com.