Head (still) in the Cloud

A buyer's guide to cloud

KEMP LITTLE

KEMP LITTLE

Contents

A buyer's guide to cloud

By 2018, we have reached a stage where the term cloud is no longer new, nor revolutionary. Yet, many organisations are still asking lots of questions about it: What are the latest cloud models? How can we better use the cloud to maximise its benefits and save costs? Has the IT world finally overcome the traditional problems that existed with cloud such as speed and security? What are the legal risks and issues that our organisation would face in the cloudsphere? For better or for worse, we still have our heads in the cloud, some twenty years on from the rise of cloud computing.

The answer to some of these questions may not be as clear-cut as the simple fact that the uptake of the cloud by many organisations is still rising. In the third quarter of 2017 alone, Amazon Web Services ("**AWS**") reported $4.58 billion in revenue, accounting for 10 per cent of Amazon's total revenue for that quarter.[1] In late 2017, Gartner projected that worldwide public cloud services would grow by 17.5 per cent between 2017 and 2018, to total US$305.8 billion.[2] Gartner predicts a five-year growth rate of 16.6% through to 2021 in cloud services, with IaaS leading the segment at 36.6% in 2017.[3]

Despite the cloud being now a relatively 'aged' concept in the IT world, IT modernisation, cost efficiencies and innovation in the cloud space itself continue to drive up the growth of cloud adoption, and urge cloud providers to come up with new and innovative cloud models for customers. However, as organisations adopt the cloud more frequently and quickly, a lack of clarity and consistent opinion as to the perceived risks of cloud services can be problematic for both providers and consumers of cloud services when contractually allocating legal and commercial risk, especially when a key driver towards the cloud for many organisations in today's economic climate is the need to control costs.

[1] https://www.cnbc.com/2017/10/26/aws-earnings-and-revenue-q3-2017.html
[2] https://www.gartner.com/newsroom/id/3815165
[3] https://www.gartner.com/doc/3803517

1 Cloud computing… back to basics

1.1 What is the cloud

Despite some of the cloud terms now being (almost) household concepts, it is probably useful to go over some of these terms, and mention any updates that may have been made.

In very simple terms, cloud computing is the practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than infrastructure stored locally or on a personal computer. In simple terms, anyone with a Gmail account is using a cloud service.

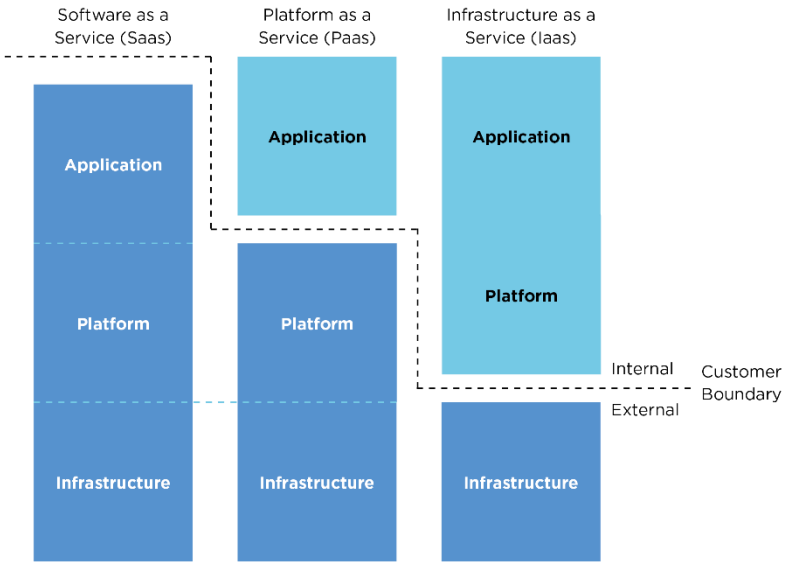
Cloud computing services form part of the service based computing trend, which consists of the more traditional IT outsourcing, as well as application service developments (and we focus on this in this section describing application service developments (ASPs), Software as a Service (SaaS), common types of cloud-computing and onwards. The similarities and differences is these services are important factors in determining an approach to the allocation of risk and responsibility in commercial terms.

1.2 Application Service Provision ("ASP")

The first evolutionary step towards cloud computing took the form of ASP. ASP is the process whereby software that was traditionally run and accessed from an organisation's on-site servers is moved to a supplier's server at an offsite location. A communication link would be established between the organisation's IT infrastructure and the supplier's offsite location. The software usually being subject to a similar licensing and update release regime as if the software was still being hosted locally.

1.3 Common types of cloud computing

The most common types of computing services that are widely talked about as "cloud computing" are Software as a Service, Platform as a Service and Infrastructure as a Service. Each of these has a varying degree of reliance on the customer's own internal infrastructure. The following diagram shows the split between internal and external infrastructure under each of the different cloud models:



The available cloud offerings in the market

1.3.1 Software as a Service ("SaaS")

SaaS shares a number of similarities with ASP in that the software is run and maintained on the IT supplier's servers and is accessed by the customer remotely over the internet, usually through a web browser. SaaS differs from ASP however in that it is designed to be accessed only over the internet. It is also designed as a "one to many" model meaning the software and its associated host hardware can be used to serve a number of customers simultaneously.

This "one to many" model means SaaS benefits from faster and more extensive development and feature updating. Unlike traditional software licences, SaaS is typically priced on a periodical, per seat or per user basis, scaled according to service features, resilience level and storage space. In accessing software in this way, a customer does not need to buy/licence, install or run the software on its own computers and so eliminates the need to maintain or update the software.

Additionally, unlike more traditional software offerings where there is a high degree of supplier customisation to meet customer requirements, in SaaS, the customer typically has to adapt their requirements to meet the supplier offering.

The advantages of SaaS are:

- It is cheaper than ASP as there are minimal configuration costs. SaaS is designed to be run and accessed remotely and, unlike ASP, there is no time and cost needed to "move" local software and configure it to operate remotely.

- Reduction in on-going maintenance and support costs. The “One to Many” model (i.e. multiple customers of the SaaS solution utilising the same software/hardware) means economies of scale can be achieved for maintenance and support.
- The costs of keeping “up-to-date” are reduced. As the customer does not have control of the software and the hardware it runs on, the supplier can roll out new versions and updated features on a regular basis to all customers simultaneously.
- Widely adopted SaaS solutions are more likely to have standardised contractual terms which can reduce procurement timescales.

1.3.2 Platform as a Service (“PaaS”)

This is the delivery of IaaS with the addition of a runtime environment/operating system being provided by the supplier. This allows a customer to run software on an IT supplier’s servers within the pre-configured virtual operating system. Under PaaS, a customer has little to no control of the underlying operating system and hardware resources. Unlike IaaS, it is the supplier which is responsible for the provision and maintenance of both the operating system and the underlying hardware. The customer is only responsible for selecting and managing the software that is run on the virtual operating system. Microsoft’s Windows Azure is an example of PaaS.

1.3.3 Infrastructure as a Service (“IaaS”)

This provides a customer with remote access to certain preconfigured hardware which the customer is able to control and use as if it had access to the same physical hardware on-site. A common IaaS offering is a “virtual server” which allows a customer to use the functionality of a traditional server as if it had access to a physical server of the same technical specification.

The term “virtual server” is used as the customer is not accessing an individual instance of hardware located at the IT supplier’s premises, rather it is using a set proportion of the shared resources of a powerful data centre. In this form of IaaS, the supplier is only responsible for the maintenance and running of the “virtual server” and its underlying hardware. The customer is responsible for running and maintaining the operating system and all software and applications running on the “virtual server”.

Cloud Storage is an obvious example of this, where a customer stores and retrieves its data from an IT supplier’s servers, rather than storing and retrieving it from its own internal infrastructure (e.g. in Amazon’s offering this is called “simple storage service”, or “S3”).

The advantages of IaaS are:

- The same as for SaaS, but on a larger scale. There is a reduction in infrastructure investment, maintenance, refresh and running costs for every element of IT infrastructure which are accessed remotely over the internet having, previously been physically present on-site.

1.3.4 The emerging new 'hybrid' cloud

Hybrid cloud is the new emerging model for businesses that operate a mix of their own infrastructure (i.e. private cloud) mixed with the services of a public cloud services provider such as Amazon or Google. The public and the private cloud communicate through an encrypted connection that ports the information and applications between the two clouds. The cloud space usually runs some type of cloud management platform to effectively connect with the public cloud space (for example, NemakiWare, which is an open source enterprise content management software).

The two clouds are very distinct elements, which provides organisations with significant flexibility because they can store sensitive data on the private cloud, while being able to utilise the resources of the public cloud to use applications necessary for the processing of the data that may be stored on the private cloud; in a way, this provides organisations with the very best of both worlds.

The hybrid cloud is increasingly popular with organisations in the financial sectors. The ability to place orders through a private infrastructure, but using the public cloud to run analytics saves a great deal of space for dealing with latency-sensitive trade orders; for many investment firms, the ability to store confidential algorithms locally, while having the ability to use the public cloud for certain computational needs is highly desirable. Similarly, the model is gaining ground within the health and legal sectors.

Among the benefits of using a hybrid cloud model are:

- direct accessibility means reduced latency and delay: reliance on the speed and availability of the internet poses a great risk for organisations. Being able to access data locally, while also having the ability to utilise the public cloud bears great benefit for organisations with time-critical needs.

- ability to call on backup capacity from the public cloud: organisations with a locally stored private cloud can cater for their computational needs locally and under ordinary circumstances, while being able to rely on additional space and capacity within the public cloud.

- paying for what you need: being able to call on additional resources on a needs-only basis means that organisations do not incur the cost of building additional capacity locally for one-off requirements and only pay for additional public cloud capacity as and when needed.

However, the hybrid model suffers from a number of issues, some of which are known to the public cloud model:

- **data security**: the transfer of data between the public and private cloud spaces still opens up the data to being tapped by a third party and therefore, poses the same risks as data stored within the cloud space.
- **cost**: organisations with small budgets would still need to deploy private infrastructure – for organisations looking to the cloud purely to save money, the hybrid model poses this aged issue.
- **suitability for time-critical needs**: the hybrid model, much like the public cloud, is still ill-suited in dealing with circumstances where the transfer of data at both ends is time critical for organisations, and delay and latency are not an option.

According to a report by Gartner, the mainstream adoption of hybrid cloud is still some time away – in 2015, Gartner predicted that it will take two to five years for organisations to start to adopt hybrid on a mainstream basis. This goes to show that organisations are still trying to determine the exact level of cloud that they need for their business to maximise cost savings.

2 Statutory/regulatory issues

Cloud computing arrangements raise a variety of issues for the lawyer relating to the application of statute, regulations and contractual terms. Many of these are not specific to cloud computing but apply more generally to many types of technology services agreements.

Statutory/regulatory issues

There are some issues raised by statute and regulation which have a particular prominence in cloud-sourcing arrangements. Those are:

- the Data Protection Act 1998;
- EU's General Data Protection Regulation (the "**GDPR**");
- MiFID/SYSC rules (where relevant);
- FCA guidance on outsourcing to the cloud; and
- the European Banking Authority Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulations (EU) No 1093/2010.

2.1 Data Protection Act 1998

The Data Protection Act 1998 (the "DPA") provides a number of protections for individuals regarding any data which identifies them (what is known as "personal data" under the DPA). Those who control the processing (meaning storing, recording, transmitting, etc.) of personal data must comply with the eight Data Protection Principles (the "Principles") contained in Schedule 1 of the DPA (as well as a number of other provisions).

Large amounts of unfiltered information are generally transferred to, or stored by, a third party provider in the cloud-sourcing context – for example where a cloud-sourcing email service is provided. It is almost inevitable that this type of arrangement will mean the transfer and/or storage of large amounts of personal data between the customer and the provider. Users of cloud-sourcing arrangements will need to ensure that their agreements with their cloud-sourcing provider comply with their obligations under the DPA and Principles. The following table shows how these key principles have an impact on cloud providers:

2.1.1 First principle

Personal data must be processed fairly and lawfully. Whilst a number of caveats exist, usually consent of the individual must be obtained in order to process the personal data. Consent can generally only be given when an individual has been provided with sufficient information to make an informed decision.

2.1.2 Seventh principle

Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing or accidental loss or destruction of personal data. It is likely that in almost all cloud-sourcings, adequate security measures must be used to protect personal data to comply with this Principle. Where data is spread over a number of locations this may be harder to practically achieve and enforce.

Of course, this particular principle is now further strengthened by the new requirements under the GDPR, which in a number of ways, advance this particular requirement for cloud operators. This includes for example, the requirement under the GDPR for the cloud providers to specify the features of the service, including how a service is delivered and the rights and obligations of the customer in the agreement.

2.1.3 Eighth principle

Personal data must not be transferred to a country outside of the European Economic Area ("EEA") unless that country ensures an adequate level of data protection.

If personal data is to be transferred or stored (in whole or part) outside of the EEA, then that in itself is a potential breach of the DPA without certain conditions being met. The European Commission has established a formal procedure for certifying countries which have in place adequate data protection rules, however this list is small and is limited to countries such as Switzerland, Argentina and the Isle of Man.

Cloud computing issue: Cloud-sourcing is currently being predominantly offered by providers based in the USA. Organisations based in the UK (or EEA) need to ensure that any cloud services used will be provided from within the EEA or a certified country or that other methods to ensure compliance with this Principle are met.

2.2 The GDPR

The new requirements under the GDPR will have a significant impact on cloud services providers; the reason being that under the current EU Data Protection Directive (95/46/EC – the "**Directive**"), the majority of the responsibilities rested with the data controller rather than the data processor; the vast majority of cloud services providers were classified as processors, processing data at the request of the controller. The GDPR now changes this by expanding the scope of the application of the data protection rules to also catch processors. Importantly, processors are now jointly and severally liable for compensation claims made by individuals.

There are a number of changes proposed under the GDPR, which will now apply to cloud services providers. In any processing, the controller must use processors that provide 'sufficient guarantees to implement appropriate technical and organisational measures'. Further, any contracts between a controller and a processor must include the following details:

- scope, nature and purpose of processing

- duration of the processing; and
- the types of personal data and categories of data subjects.

This means that the cloud services provider and its customer must implement technical and organisational measures to ensure that the risks to any data being processed are managed.

The GDPR also imposes a number of additional obligations on cloud service providers in their capacity as data processors, including requiring that they:

- only process personal data on documented instructions of the customer (as the controller), including when it concerns international transfers;
- define the specifics of the cloud service, how it is delivered and the rights and obligations of the customer (as the controller) in the controller-processor contract;
- implement and maintain appropriate technical and organisational measures to keep the data secure;
- only use a sub-processor (i.e. a subcontractor) with the specific consent from the customer;
- make all necessary information available to the customer in order to demonstrate compliance with its data protection obligations, and allow for audits and inspections;
- assist the customer with requests from individuals, exercising their rights to access, rectify, erase or object to the processing of their personal data;
- implement incident management measures such that it is able to notify the customer as and when it becomes aware of any security incidents or breaches; and
- return or delete personal data at the end of the agreement.

A new code of conduct on data protection published by Cloud Infrastructure Services Providers in Europe (CISPE), a coalition of cloud infrastructure providers, was published in January 2017[4], which explains in practical terms how cloud service providers ought to comply with the requirements of the GDPR.

[4] https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

2.3 MiFID/SYSC rules

Regulated entities are likely to be bound by the provisions of Markets in Financial Instruments Directive[5] ("MiFID") as applied in the UK. As part of the implementation of MiFID obligations in the UK the FCA has issued the Senior Management Arrangements, Systems and Controls' ("SYSC")[6] Rules. SYSC Rule 8 applies predominantly to regulated businesses that outsource an operational function that is "business critical" to the performance of their regulated activities, e.g. their investment management or insurance sales functions. Where SYSC Rule 8 applies, that business must ensure that their agreement with the outsourced service provider contains (amongst other things) provisions that:

- protect any confidential information relating to clients;[7]
- allow them to terminate the agreement without an impact on the continuity and quality of any service provision to its customers;[8] and
- allow the regulated firm, its auditors, the FCA and any other relevant competent authority to have effective access to the data related to outsourced activities, as well as to the business premises of the service provider.[9]

Cloud computing issue: Some of these SYSC Rules are not easily workable in cloud-sourcing arrangements – for example where an application for managing investment portfolios is purchased via a SaaS arrangement. Allowing access to cloud-sourcing premises may not be practical or even feasible where data may be stored in ever-changing locations across continents. Additionally, it may be impossible to tell exactly where all data is effectively being held at any one time to make provision for adequate and effective exit/transition provisions on the termination of an agreement.

Many of the outsourcing requirements under the SYSC Rules seem practically unworkable in the general cloud-sourcing context. Their effect would be to significantly limit many of the business practices that generate the cost savings that make cloud-sourcing an attractive option; the FCA has now provided some guidance on this, and in fact, solidified some of the SYSC requirements as being applicable to the cloud (see section 2.4 below).

2.4 FCA guidance on cloud

In July 2016, the FCA finalised guidance for firms outsourcing to cloud and other third party IT services (the "**Guidance**"). In this Guidance, the FCA, in effect, gives a green light to banks to use cloud services, but clarifies that it considers cloud services

as an 'outsourcing', therefore extending the application of the FCA rules around outsourcing to the cloud. As such, the Guidance builds on and consolidates the

[5] Directive 2004/39/EC of the European Parliament and of the Commission of 21 April 2004.
[6] http://fsahandbook.info/FSA/html/handbook/SYSC.
[7] SYSC Rule 8.1.8(10).
[8] SYSC Rule 8.1.8(7).
[9] SYSC Rule 8.1.8(9).

requirements in SYSC (vis-à-vis banks) and Directive 2009/138/EC ("**Solvency II regulations**") when it comes to cloud-sourcing.

The Guidance provides specific requirements in respect of the following issues:

- **Legal and regulatory considerations:** this requires customers to take certain clear steps before entering into an agreement with a cloud provider, including regarding their business case, due diligence risk assessment, accurate records, understanding where data is stored and clarify on data protection obligations.
- **Risk management:** this requires customers assess outsourcing risks and identify best practices.
- **International standards:** customers are required to assess the suppliers' compliance with international standards.
- **Oversight of supplier:** customers are required to vet the supplier in respect of clarity of responsibility, sufficiency of skills, management of exit and transfer provisions and dispute measures.
- **Data security:** customers are required to undertake data risk assessments, obtain and understand data loss and breach notification processes and consider data segregation (particularly in the public cloud). Customers are encouraged to agree a data residency plan with the provider to specify the jurisdictions where the data will be stored, processed and managed.
- **Effective access to data:** This is effectively to ensure unhindered access by regulators to the data, as and when needed, disallowing any inhibition of "effective access" in any jurisdictions.
- **Access to business premises:** right of access should be unlimited, and it should only be restricted in limited circumstances. The Guidance does acknowledge that there may be legitimate cases of limitation of access such as data centres, but unhelpfully states that there equally will be cases where access to data centres will be required. The perceived wisdom here is that provisions for access must be made, but clear limitations and prudent controls should be in place.

2.5 The EBA on cloud[10]

The European Banking Authority (the "**EBA**") has recently issued draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010[11] (the "**Draft Recommendations**") to respond to widespread uncertainty regarding the supervisory expectations that apply when outsourcing to cloud service providers which in itself forms a barrier to financial institutions using the cloud. While the recommendations are not binding, they reiterate

[10] https://www.eba.europa.eu/documents/10180/1848359/Draft+Recommendation+on+outsourcing+to+Cloud+Service++%28EBA-CP-2017-06%29.pdf
[11] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1093&from=EN

Article 16(3) of Regulation (EU) No 1093/2010 that financial institutions must make every effort to comply with them.[12]

The Draft Recommendations have applied a more holistic approach to discussing requirements for cloud and do not distinguish between the different types of cloud (e.g. SaaS v IaaS). They provide detailed guidance on the following key areas:

(1) Materiality assessments

Prior to engaging a cloud service provider, financial institutions should self-assess what activities are 'material', this is done by considering the criticality and interest risk profile of the activity, the impact of outages, disruption, confidentiality and data breaches. Financial institutions should provide the competent authority (in the UK, the FCA) with details of each cloud service provider, the contract governing the relationship and certain other details that may be requested by the competent authority. Finally, the financial institution should maintain an updated register for both material and non-material outsourced activities at both institution and group level.

(2) Access and audit rights

The Draft Recommendations adopt a split approach with different rights for the financial institution and component authority.

Competent authority:

The competent authority should be afforded full access to the cloud service providers' business premises and devices, systems, networks and data used for providing the outsourced service, this right should not be impeded by contractual arrangements but the competent authority should provide reasonable notice prior to onsite visits unless such notice is not possible due to an emergency. As final points, all audits should be carried out by staff with the requisite skills to understand the technical complexity of the services and cloud service providers should at all times cooperate with ongoing audits.

Financial institutions:

It is recommended that financial institutions are also afforded the access rights above, however, the Draft Recommendations take a proportionate approach and institutions may instead opt for; (i) pooled audits performed jointly with other clients of the same cloud service provider; or (ii) third party certifications / internal audit reports provided the certification or the report meets certain specific requirements relating to its quality and relevance.

(3) Security of data and systems

Prior to outsourcing, financial institutions should classify their activities and related data and systems to understand required protections, conduct a risk based selection

[12]https://www.eba.europa.eu/documents/10180/1848359/Draft+Recommendation+on+outsourcing+to+Cloud+Service++%28EBA-CP-2017-06%29.pdf

of them in order to consider which should be outsourced to the cloud and pre-define appropriate levels of data protection, confidentiality, continuity of service, integrity and traceability of data and systems.

The draft recommendations make special mention of agreements undertaken outside of the EEA, where a risk based approach needs to be taken with regards to assessing political and security stability of jurisdiction, governing law, enforcement procedures and insolvency procedures.

(4) Chain outsourcing (subcontractors)

Subcontractors should be obliged to fully comply with the obligations imposed upon the cloud service provider. Cloud service providers should also retain full responsibility and oversight over subcontractors and specify certain types of activity that are excluded from subcontracting.

To require consent to change each subcontractor would be overly burdensome, however, contracts should impose an obligation on the cloud service provider to notify financial institutions of any significant changes to their subcontractors and the notice period duration should allow the institution to carry out a risk assessment. Crucially, contracts should feature a clear termination right if subcontracted services will have an adverse impact on the financial institution's risk assessment.

(5) Contingency plans

Plans should include a clearly defined exit strategy and termination and exit management clauses in contracts to allow outsourced activities to be transferred to another service provider or insourced. Institutions should ensure such plans are comprehensive, documented and tested. They should also identify alternate solutions and develop transition plans to ensure continuity of services. Finally, contracts should contain an obligation on cloud service providers to cooperate with an orderly transfer of the activity to another provider.

2.6 Network and Information Security Directive

On 6 July 2016, the European Commission Directive on Security of Network and Information Systems (the "**NIS Directive**") was adopted by the European Parliament, and in early 2017, was confirmed to be implemented by the UK Government, despite the Brexit vote. The NIS Directive applies, broadly, to two categories of market players, including certain digital businesses such as online marketplaces, cloud computing services and search engines.

Based on the NIS Directive, cloud operators will have to take appropriate security measures and notify significant incidents to the relevant national authority. Cloud service providers adopting security measures must ensure that the security measures are appropriate for the particular circumstances, including:

- technical and organisational measures that are appropriate and proportionate to the risk;

- measures that should ensure a level of security of network and information systems appropriate to the risks; and
- measures that should prevent and minimise the impact of incidents on the IT systems used to provide the services.

Cloud services providers must also take the following into account when implementing security measures, including security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing and compliance with international standards. Under the new directive, cloud service providers are also required to report serious security incidents to their relevant national authority; the directive contains the relevant factors that are to be taken into account by cloud service providers when determining when an incident is considered to be serious.

Cloud computing issue:

For cloud computing providers, the new obligations will require strengthening and adapting certain existing infrastructure. The resilience of cloud computing networks will increasingly come under scrutiny as cybercrime and incidents of hacking continue to rise. Business leaders, along with the public, are likely to become more security conscious regarding storing their data online. Developments in the implementation of this cybersecurity legislation will undoubtedly have knock-on effects for service providers and users in the cloud computing sphere.

3 Contract issues

As with any contract for the supply of services, the key legal and contractual issues for a cloud deal will very much vary according to the services being offered and the requirements of the customer. The following however are a number of issues which should be considered as to why traditional IT outsourcing contract clauses might not always be suitable:

3.1 Outsourcing versus cloud

In the below table, we set out the main differences from a contractual approach perspective to the different issues under outsourcing and cloud contracts.

IT Outsourcing	Cloud
Service Performance	
In outsourcing deals, customers often push to secure supplier warranties of service performance against specifications or requirements, e.g.: *"The Service Provider represents, warrants and undertakes that throughout the term:* *(a) the service shall meet all the requirements set out in Schedule 4 (The Customer's Service Requirements);"* This is linked to the above mentioned point that in an outsourcing, the supplier is offering a customised service which is especially adapted to match the customer's specifications. In addition, customers typically look for warranties relating to the standard of performance of the service e.g.: *"It shall discharge its obligations pursuant to this agreement with all due skill, care and diligence including Good Industry Practice and (without limiting the generality of this clause) in accordance with its own established internal procedures."*	In cloud deals, the nature of the "one to many" model means cloud services are not usually highly adapted to the customer's requirements outside a clearly defined set of parameters. This less flexible approach is reflected in the warranties that a cloud supplier may therefore be prepared to offer. Typically cloud suppliers will only offer limited warranties of performance, often confined to providing the cloud services in accordance with "good industry practice" or "reasonable skill and care". The reality therefore is that a customer may have to rely on a performance warranty based around words such as "reasonable" and "good industry practice" even though it is difficult to understand and advise on what "reasonable" and "good industry practice" mean in such a varied and immature marketplace.

Compliance with Applicable Laws	
Within many IT agreements the supplier will give a warranty that it will comply with applicable laws. This is often seen as an almost "boilerplate" provision in an IT outsourcing deal e.g.: "*The services shall be performed in compliance with all applicable laws.*" This is because, it will often be quite a straight forward question as to what laws are to apply to a supplier in the performance of its obligations under the agreement as the locations of service performance are set (and so the applicable laws can be quickly determined).	The same question in cloud deals is not so straight forward. Where, for example, will the cloud services be provided from? Will the provision of the cloud services involve the use of the supplier's equipment in a number of different jurisdictions? Is the customer's data being transferred both into and out of EEA jurisdictions raising data protection issues? It should be evident therefore that in cloud contracts, the question of compliance with applicable laws is not so straightforward. Customers should carefully check to what extent the supplier is warranting that the services will comply with applicable law and whether for example, such a warranty is limited to the provision but not receipt of the services. It may be that a promise of compliance with the laws of where the supplier's servers are based, and where the service is provided from (which can be anywhere globally and often will be in lesser-developed nations where resource/environment costs are lower), doesn't meet the customer's requirements of compliance with applicable laws where the services are actually accessed by the customer.
Limits on Liability	
Typically, customers in an outsourcing will push to have a limit on the supplier's liability based on a multiple of the charges. For operational (as opposed to	Cloud suppliers have: ▪ less implementation/transition project work where generally

implementation) outsourcing phases this will be a calculation of charges based over a year – reflecting the steady-state and long-term nature of the service provision e.g.: *"The aggregate liability under this agreement (whether in contract, tort, negligence or otherwise) of: Supplier to XXXX for any event or series of connected events shall in no event exceed the greater of:* *(a) £[ ] ([ ] pounds); and* *(b) [200]% of the charges paid and payable by XXXX for the services during the year of the agreement in which the event or series of connected events first occurs;"*	margins/pricing are more profitable for them; and ▪ shorter term deals for less money; so are less minded to offer multiples of charges of limits on their liability as the risk doesn't match the reward.
Exclusion of Losses	
Limitation of liability and exclusion of losses clauses can differ significantly, not only between IT outsourcings but also between different types of cloud contracts. It is not always possible to draw a distinction between outsourcing and cloud deals due to such a high degree of variance. That said, a standard IT supplier exclusion of loss clause might read: *"XXXX shall not be liable to client for any damage to loss of or corruption of software or data, loss of profit, production, contracts, anticipated profits, revenues, anticipated incidental, punitive or consequential loss or damage."*	Certain heads of loss which are often excluded by a supplier in an IT outsourcings may not be suitable in the cloud context. ▪ Loss of data (on a direct and indirect basis) is often excluded by a supplier as a recoverable loss in a wide array of IT contracts. In the cloud context, is this suitable? Due to the "as a service" nature of cloud, will not almost everything to do with the services involve transmission of the customer's data? If for example, a cloud provider is offering cloud storage services, is it appropriate for the provider to be excluding liability for loss of

	data? In reality this is likely to be one of the most significant losses for a customer if there is complete service failure. ▪ Anticipated savings is another type of loss which is often excluded in IT contracts. Cloud services however are often adopted by customers due to the cost saving benefits that can be achieved by moving away from traditional IT infrastructure. If a primary purpose of a customer entering a cloud contract is to achieve cost savings, and if a supplier is marketing a cloud service on the basis that such savings can be achieved, should it follow that anticipated savings are excluded as a recoverable loss within a cloud contract? Any form of contract which transfers a service performance obligation to a supplier which was previously undertaken by a customer internally, means that a customer is trusting a supplier to do something which will reflect badly on the customer (and a lot less so on the supplier) to the wider world if it fails. There are some examples to date where cloud service providers have had significant failures but the customer has taken the significant damage to their goodwill and reputation. Use of new service offerings by a customer, especially one where security and integrity issues are publicly discussed, may mean that goodwill and reputational damage to customers could be greater, yet typical clauses will remove

	any opportunity to recover these types of losses where the supplier is in breach. However, as in most other commercial agreements, whilst the customer risk might be higher there is little evidence to date that any supplier will be prepared to offer goodwill or reputational losses as a recoverable head of loss under contract for cloud-services. This is a customer risk that customer's need to be prepared to carry.
Third party IPR Infringement	
In a bespoke outsourcing services agreement, it is common to expect the supplier to provide the customer with an indemnity such that it will fully indemnify and hold harmless the customer for any costs and actions arising out of any claim that the customer's use of the services infringes any IPR of any third parties. A typical indemnity for this would likely read: *"Supplier shall indemnify Customer and its Affiliates against all claims, demands, actions, costs, expenses, losses and damages arising from or incurred by reason of any infringement or alleged infringement (including the defence of such alleged infringement) of any Intellectual Property Rights in connection with the provision or receipt of the Services or the use or possession of any information technology, Deliverables and/or any Project-Specific IPR provided or made available to Customer or any of its Affiliates under or in connection with this Agreement."*	This has been less of an issue in the cloud context where the risk of third party IPR infringement has been perceived to be a lesser risk. As such, the standard position for cloud providers has been to not offer this indemnity. In recent times, there has been a growing pattern of patent trolls (companies whose sole function it is to find patent infringement and enforce it) to enforce third party patent infringement against cloud services providers, as well as their customers. To combat this, Microsoft has become the first company to offer a third party IPR infringement indemnity to all of its cloud computing customers to cover any legal risks arising from the open source software used in its Azure cloud computing service. Microsoft has also announced that its customers could benefit from 10,000 of its

	patents when defending themselves against such legal attacks. This growing trend, coupled with Microsoft's latest response, mean that it is completely valid for customers to push for an indemnity against the risks of third party IPR infringement within the cloud service.
Confidentiality	
Confidentiality is a good example of almost standard "boilerplate" clauses in IT outsourcing agreements which might not work quite as drafted in a cloud computing agreement. Confidentiality provisions will commonly express obligations that certain types of information will be protected as confidential. Typically, such clauses will make clear that such a contractual duty of confidentiality does not apply where the information is already in the public domain e.g.: *"The obligations set out in this clause 12 shall not apply to confidential information which the receiving party can demonstrate: (a) is or has become publicly known other than through breach of this clause."*	Where data is transmitted via a non-secure network e.g. the internet, this could be considered as being akin to it becoming publicly known or being in the public domain – at which point certain types of confidentiality clauses would no-longer impose a contractual duty of confidence on the data. This issue of course turns on the precise drafting of the clause, however this highlights why "boilerplate" clauses from IT outsourcing agreements need to be closely scrutinised to determine whether such clauses correctly function in a cloud computing context.
Service Levels	
Outsourcing service levels attempt to give customers confidence that the totality of the service they have outsourced to a supplier will be performed to a level that is acceptable. Often the customer will look for an overall "end-to-end" service	Where service provision is entirely over the internet, any service level that measures the availability of the internet is entirely dependent on internet performance for the measurement of the "end-to-end"

level, often this will include "Availability" measures targeting the level at which the customer expects the service being contracted for to be available.	service availability. The last few years have seen numerous high profile examples where internet availability has been effected by factors no supplier of cloud services would take responsibility for, be it: ▪ political unrest;[13] or ▪ accidents cutting submarine telecommunication cables.[14] To date that has meant very few cloud service providers giving availability of service levels that take responsibility for internet performance. As the infrastructure and routing of the internet gets better understood and more resilient this is likely to change, and there are examples of large providers looking to provide 99.9% uptime SLAs.
Audit	
A requirement that a customer can audit the service provider (be it the audit of a physical property or of data held) is often required as simple good practice, or if you work in regulated sectors such as financial services[15] or public sector procurement[16] it may become a legal/regulatory requirement. Typically the explicit contractual right to access and audit property/data is captured in a contract clause e.g.:	It is likely that a cloud-provider will find it: ▪ difficult if not impossible to identify the physical location of individual service provision or data storage locations for an individual customer; and ▪ impossible to allow one customer access to service provision

[13] http://www.bbc.co.uk/news/technology-12306041.
[14] http://news.bbc.co.uk/1/hi/technology/7228315.stm.
[15] Senior Management Arrangements, Systems and Controls - SYSC Rule 8.1.8 - http://fsahandbook.info/FSA/html/handbook/SYSC/8/1.
[16] OGC Model Terms and Conditions of Contracts for Services - http://www.ogc.gov.uk/Model_terms_and_conditions_for_goods_and_services.asp.

"XXXX may, not more than once in any contract year in respect of each of the following, conduct audits for the following purposes: *(a) to verify the accuracy of charges* *(b) to review the integrity, confidentiality and security of the XXXX data."*	locations without opening itself up to. Notwithstanding the above, please see the above comments on the GDPR and the requirement for cloud providers as processors to allow for audits and inspects to demonstrate compliance with GDPR requirements.
Termination/Exit	
A prudent customer outsourcing any aspect of their business will ensure that the contract with the supplier contains terms that will help guarantee that on termination or expiry of the agreement the supplier will: ▪ return information and materials that the supplier has to allow the customer to either bring services back "in-house" or transition to a replacement supplier; and ▪ provide such other information and support that the customer will need to allow a smooth transition of the service. Typically a clause might include a requirement that: *"The deliverables in relation to the exit plan shall include:* *(a) relevant available information about propriety products, tools and methods and the access to information to be provided by the service provider to the XXXX and/or a replacement service provider."*	The relative recent rise of cloud computing solutions has meant that there is no industry standard data storage format or business process in relation to the packaging, reading or moving of data. In fact a fundamental attraction of cloud based solutions – their lower costs – are dependent on suppliers being able to manage formats, database structures and locations in the most efficient way possible for them. The effect of this is that exit arrangements need to be more detailed and explicit in cloud computing. Often IT outsourcings might provide for quasi "agreements to agree" on exit plans. Cloud computing customers should not take the risk of agreeing exit arrangements post contract as there is a significant risk they could find themselves "de facto" locked-in to continuing to use a supplier for fear of not being able to appropriately transition services away from the cloud supplier.

	Customers should therefore look to agree with suppliers prior to contract signature a detailed exit plan which includes: ▪ The details of the file formats that the customer's data will be returned in. ▪ The grant of any licences needed to view/access that returned data. ▪ Provisions extending the scope of any licences to permit use by others e.g. replacement providers. ▪ Details of the method/medium by which data will be transferred e.g. will the data be made available electronically? Will the data be sent to the customer on physical media? Timescales for the transfer of the customer's data.
Policies/Standards/Security	
Whilst an outsourcing customer wishes to outsource a service provision, they want to know that the manner and behaviour of service performance is at least at the same base standard as if it was being done "in-house" in relation to issues such as IT and information security. It is therefore common to see customers requiring suppliers, especially those who are on the customer's premises or have access to the customer's systems, to agree that it will perform the services in accordance with the customer's own policies and standards e.g.:	Simplistically put, the ethos behind cloud-based solutions is that the customer's requirements (their "plug" so to speak) will be adapted to fit the supplier's service offering (their "socket"), the antithesis of the typical outsourcing offering. Because of this ethos, the argument goes, suppliers are able to offer customers the cost savings of a one-to-many offering. It is therefore difficult for suppliers to offer to comply with individual customer policies. As such compliance might require system/process/IT changes that would either impact the other

"The service provider acknowledges that it: *(a) has made itself aware as to the contents and requirements of the XXXX policies so as to ensure that it is able to comply with them during the term."*	customers who are being supported from similar delivery centres or, if they can be complied with, will be at significant extra costs. That is why, typically, suppliers will offer customers a contractual promise to meet standards and policies, but it will be the suppliers standards and policies which the customer will have to consider to determine if they meet their own requirements.

For more information please contact:

Andrew Joint
Partner, Commercial Technology
+44 (0) 20 7710 1667
andrew.joint@kemplittle.com

Ed Baker
Managing Associate, Commercial
+44 (0) 20 7710 1668
edwin.baker@kemplittle.com

Korolyn Rouhani-Arani
Senior Associate, Commercial
+44 (0) 20 7710 1675
korolyn.rouhani@kemplittle.com

This guide provides a clear and user-friendly introduction to the concept of cloud computing, by contrasting cloud computing with IT outsourcing, discussing regulatory questions, and examining questions that should be considered in relation to contracts for such IT services. The guide is intended primarily for buyers, and potential buyers, of services but will also be a valuable resource for lawyers involved in the negotiation of contracts for IT services. This guide is part of Kemp Little's series of documents on the cloud.

Kemp Little LLP is authorised and regulated by the Solicitors Regulation Authority, number OC30024. February 2018