Knowing the past to understand the present\(^1\) – issues in the contracting for cloud based services

Andrew Joint*, Edwin Baker
Commercial Technology Team – Kemp Little LLP, UK

Abstract
This article builds on our previous introductory article to cloud computing ([2009] 25 CLSR 270-274) and seeks to explain how cloud computing has evolved. We then discuss how this evolution impacts on key contractual and legal considerations and how the treatment of these considerations might differ from their treatment in traditional IT supply agreements.

© 2011 Kemp Little LLP. Published by Elsevier Ltd. All rights reserved.

1. Introduction – the rise of ‘cloud’

In 2008 Merrill Lynch estimated that by 2011 the global market for cloud services\(^2\) would have a value of around $160 billion\(^3\). By 2009 Gartner estimated that the global market for cloud services had a value of around $46 billion with a predicted rise to around $150 billion by 2013\(^4\). Regardless of whether these lofty estimates are to be believed, cloud computing use is becoming more prevalent and organisations spanning both public and private sectors are increasingly being offered cloud based solutions. There is a wide array of cloud services on offer varying from simple Software as a Service (SaaS) solutions right through to complete virtualised cloud platforms. However, the progress of the industry is facing some significant challenges, notably:

- a wide scope of cloud services coupled with a significant amount of industry jargon – often used inconsistently. Potential consumers of cloud services can often be somewhat unclear as to what exactly is on offer and how this differs from traditional IT solutions; and
- divided industry opinion as to whether the cloud is suitable for use by all types of businesses. This is aptly illustrated by quotes in two articles contained within a month of each other in Computer Weekly in the UK in 2009:
  - “Data can be safer in the Cloud than on the desktop”\(^5\); and
  - “Businesses say cloud computing a risk too far”\(^6\)

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

---

\(^*\) Corresponding author.

E-mail addresses: Andrew.Joint@kemplittle.com (A. Joint), Edwin.Baker@kemplittle.com (E. Baker).

\(^1\) To loosely paraphrase the American scientist Carl Sagan.

\(^2\) There is no settled definition as to what is meant by ‘cloud services’. In this article we use the phrases “cloud services” and “cloud computing” to mean the delivery of IT services via the internet.

\(^3\) The Cloud Wars: $100 Billion at Stake, Published by Merrill Lynch, May 7, 2008.


0267-3649/$ – see front matter © 2011 Kemp Little LLP. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2011.05.002
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.

2. Cloud: “Prediction is very difficult, especially about the future…”

The current cloud solutions being offered by IT suppliers are the latest evolutionary step in the delivery of IT, an evolution which has progressed over the last 50 years as set out in Fig. 1 below.

We see these changes as an evolutionary rise of service based computing empowered by:

- hardware developments since the arrival of the programmable computer in the 1940s;
- software developments since 1969 when hardware and software were first unbundled; and
- the rise of the internet.

Cloud computing services form part of the service based computing trend and we focus on this below describing IT outsourcings, application service provision, software as a service, cloud computing and onwards. The similarities and differences between these services are important factors in determining an approach to the allocation of risk and responsibility in commercial terms.

2.1. Early IT outsourcings

IT outsourcing is perhaps the most iconic and understood form of a supplier delivered IT service. In an IT outsourcing a customer has certain IT requirements which, rather than manage and run itself, it contracts with an IT supplier to perform on the customer’s behalf. An obvious example of this is a ‘desktop outsourcing’ where a customer contracts with an IT supplier to manage and run itself, it contracts with an IT supplier to

The key advantage of outsourcing an IT function is that a customer obtains the benefits of:

- specialised ‘skill-sets’ without the need to incur the costs of additional employees. The IT supplier will have employees with the necessary expertise to run the outsourced function effectively. The customer therefore avoids needing to employ a number of IT specialists where it might not be economical for the customer to employ staff with similar expertise on a full time basis;
- the performance of the service in exchange for a calculable service charge. This can be advantageous for budgeting purposes as an organisation’s IT needs can be satisfied for either a set charge or a known charge within certain determinable parameters. This approach can mitigate the risk of unexpected IT costs. Additionally, where a supplier is responsible for hardware upgrades/replacements, it avoids the unknown ‘peaks and troughs’ involved in the costs for refreshing IT hardware/software; and
- potentially avoiding the locking up of capital in infrastructure. Often the supplier will own the equipment used in its performance of the IT function and is effectively leasing use of this back to the customer through a service charge. This arrangement means that an organisation does not need to invest funds into the IT infrastructure, freeing such capital for other business purposes.

2.2. 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 off-site location. A communication link would be established between the organisation’s IT infrastructure and the supplier’s off-site location. The software would usually be subject to a similar licensing and update release regime as if the software were still being hosted locally.

The advantages of using software via the ASP model are:

- a reduction in hosting costs. An organisation doesn’t require the software hosting infrastructure on-site and therefore avoids the cost of purchasing, running and maintaining such hardware;
- ASP allows for customised and ‘bespoke’ software solutions to be offered remotely. ASP involves the supplier offering a customised service so that the configuration of the on-site software can be moved and operate correctly off-site. The IT supplier is therefore heavily involved in ensuring the new solution operates in an equivalent manner to the superseded solution. ASP can therefore be suitable for highly customised software deployments; and
- in a similar manner to IT Outsourcing, ASP can facilitate a transition to a simple service charge for the use of software without the associated costs of hardware and running costs.

2.3. 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 only accessed over the Internet. It is also designed on a one-to-many model meaning the software and its associated host hardware can be used to serve a number of customers simultaneously. Salesforce.com is a good example of a SaaS product.

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 levels and storage space. In accessing software in this way, a customer does not need to buy/license, 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

---

7 A quote often attributed to the Danish Physicist Niels Bohr.
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 taken 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 upgrades on a regular basis to all customers simultaneously; and
- widely adopted SaaS solutions are more likely to have standardised contractual terms which can reduce procurement timescales.

2.4 Cloud computing

Cloud computing is the next evolutionary step from SaaS. Under a cloud computing arrangement not only is the software provided remotely, but a whole range of scalable computer technology-enabled resources are provided as a service (e.g. operating system, data storage, processor resources). "Cloud computing" is often divided into a number of categories of service by IT suppliers, often the most popular being categorised as:

- **SaaS** – Software as a Service, discussed above.
- **IaaS** – Infrastructure as a Service. This provides a customer with remote access to certain pre-configured 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”. Amazon’s Elastic Compute Cloud (EC2) is an example of this form of IaaS. IaaS can also apply to discrete elements of IT infrastructure being provided as a service. 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”).
- **PaaS** – Platform as a Service. 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.
- **EaaS/XaaS** – everything as a service. This is a hybrid term referring to a combination of SaaS, IaaS and PaaS.
The advantages of cloud computing 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.

2.5. Utility computing

Utility computing is not really a development past cloud computing, more a refinement of EaaS/XaaS to the mass market. Utility computing is the aggregation and packaging up of different computing resources (input, processing, storage, programming, output, communications, etc) for supply on a metred basis, like water or another utility.

The advantages of Utility Computing are:

- that it claims all the benefits of ‘cloud’ and SaaS but is driven by the customer’s requirements; and
- ‘metered’ based pricing aids budgeting and allows IT capacity to rise and fall with use rather than requiring peak level availability all the time.

The benefits of utility computing can be most easily seen in the context of e-commerce. Online retailers may experience significant surge in the use of their website in the December sales rush. Traditionally an online retailer would need to purchase, run and maintain the IT equipment to deal with this peak demand which would be under-utilised for most of the year. The utility computing model allows the online retailer to only “use” the IT resources it needs at any given moment meaning it uses and pays for the means to deal with increased customer demand for only a small part of the year.
3. Are IT outsourcings and cloud services the same thing?

The evolutionary nature of the technical developments of cloud computing can be misleading when looking at the contracts for cloud services. Evolving a standard IT contract to be used for cloud based services is not necessarily a useful approach. In contrast to the evolution of the IT services they govern, a revolution in contractual clauses and a large upheaval from traditional IT contract precedents is far more realistic for certain aspects of cloud services contracts.

However, a customer that switches from using IT infrastructure on-site and in the traditional sense, to using cloud services, is utilising a form of IT outsourcing. The similarities are also not only confined to the conceptual level as both IT outsourcing and cloud service deals:

- focus on the performance of the services being provided by the supplier, and at the contractual level will likely involve a service level/service credit regime, and will contain exit provisions for dealing with transition of the services either back to the customer or to a third party provider upon the contract terminating/expiring;
- aim to achieve efficiencies and reduce costs at levels which the customer is unlikely to achieve due to the customer not having the supplier’s expertise;
- avoid/reduce the extent the customer’s capital is ‘locked up’ in IT infrastructure;
- involve the remote provision of services (although this can vary to a lesser or greater extent in the context of IT outsourcings dependent on whether this involves offshoring/onshoring); and
- are typically embodied in a contractual structure which contains a significant level of detail.

As there are significant overlaps between the scope of IT outsourcings and cloud services a corresponding overlap of the contractual, legal and commercial considerations can also occur.

However, there are fundamental differences between the two which mean a standard IT outsourcing approach will not necessarily ‘work’ in the approach to cloud service deals. This is because:

- outsourcing is typically a highly customised service tailored to the customer’s requirements and specifications. Cloud services on the other hand operate on the basis of a one-to-many model. While these services are customisable to a degree, as cloud services are a commodity service the customer may need to alter its requirements or make certain changes to these necessary to meet the supplier’s cloud services on offer. A cloud supplier will not typically customise the service for each customer beyond certain set parameters;
- in an IT outsourcing, the supplier is responsible for delivery and key performance indicators relating to this form part of a service level agreement. Cloud services on the other hand are more concerned with “availability” than delivery. The definition of a metric of availability also needs to be scrutinised in a way which may not arise in an outsourcing - does the supplier or the customer take the risk of internet problems (i.e. circumstances outside either party’s control) impacting on the availability of the services and how are service levels dealt with in such a scenario?
- in an IT outsourcing, assets and staff may transfer from the customer to the supplier either as a result of the terms of the contract or due to the operation of the Transfer of Undertakings (Protection of Employment) Regulations 2006 (“TUPE”). As a consequence, an IT outsourcing contract will contain detailed provisions dealing with such transfers and apportioning related liability and risk. Conversely, a cloud service deal will not typically involve the transfer of assets and staff nor the application of TUPE;
- in an IT outsourcing, pricing payment models can be extremely varied ranging from annual fees to complex pricing models involving concepts such as gainshare and benchmarking. In a cloud service agreement payment models are usually much simpler to calculate and may be charged on a ‘pay per use’ basis. While the cloud service calculations tend to be simpler than those found in IT outsourcings, this may nonetheless create a different type of challenge. It may not be immediately obvious or easy for the customer to estimate what the annual cost of the cloud services will be and ascertain the extent of the cost saving which will be achieved by utilising the cloud services;
- IT outsourcings may involve service development provisions which seek to enhance/improve the services over the term of the contract and the parameters for these may be agreed at the outset. Developments and improvements to cloud services on the other hand are normally made available to the customer at the discretion of the supplier as and when these are developed. A cloud service deal has less scope therefore for agreeing future functionality by a predefined stage in the contract; and
- IT outsourcing deals are typically longer, more complex, and higher value. Cloud services deals on the other hand tend to be for shorter terms, less complex and for lower values. While this is slowly changing as the market for cloud services matures, this lower value, shorter term limits the degree to which suppliers may be prepared to negotiate highly customised contractual terms for a cloud services deal.

In light of these differences, approaching a cloud service deal as a traditional IT outsourcing will not be appropriate for all aspects of the contract.

4. The mismatch of IT outsourcing clauses to cloud contracts

As with any contract for the supply of services, the key legal and contractual issues for a cloud deal will 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 contract clauses might not always be suitable:
4.1. Service performance

4.1.1. The IT outsourcing approach
In outsourcing deals customers often push to secure supplier warranties of performance of services against specifications or requirements e.g.:

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.:

4.1.2. Cloud-computing issues with that approach
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 “skill” and “care”.

The reality therefore is that a customer may have to rely on a performance warranty based around words such as “care” and “good industry practice” even though, in such a varied and immature market-place, it is very often only possible to provide generic advice on what “care” and “good industry practice” mean without disproportionately costly legal support.

4.2. Compliance with applicable laws

4.2.1. The IT outsourcing approach
Within many types of IT agreements the supplier will give a commitment (whether expressed as a warranty or an undertaking) that it will comply with applicable laws e.g.:

This is because it will often be quite a straightforward 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).

4.2.2. Cloud-computing issues with that approach
The same question in cloud deals is not so straightforward. 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 EU jurisdictions raising data protection issues?

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 the service is provided from (which can be anywhere globally and often will be in lesser-developed nations where resource/environment costs are lower and legal systems differ substantially to the UK) doesn’t meet the customer’s requirements of compliance with applicable laws where the services are actually accessed and used by the customer.

4.3. Limits on liability

4.3.1. The IT outsourcing approach
Typically customers in an IT outsourcing will push to have a limit on the supplier’s liability based on a multiple of the charges. For operational (as opposed to implementation) outsourcing phases this will be a calculation on charges based over a year – reflecting the steady-state and long-term nature of the service provision e.g.:

29.4.1. Supplier to 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 for the Services during the year of the Agreement in which the event or series of connected events first occurs;

4.3.2. Cloud-computing issues with that approach
Cloud suppliers have:

- Less implementation/transition project work where generally margins/pricing are more profitable for them; and
- Shorter term deals for less money;

so are less minded therefore to offer multiples of charges of limits on their liability as the risk doesn’t match the reward.
4.4 Exclusion of losses

4.4.1 The IT outsourcing approach
Limitation of liability and exclusion of losses clauses can differ significantly, not only between IT outsourcing but also between different types of cloud contracts. It is not always possible to draw a distinction between outsourcing and cloud deal due to such a high degree of variance. That said, a standard IT supplier exclusion of loss clause might read:

```
6.3. [redacted] shall not be liable to Client for any damage to loss of or corruption of software of data, loss of profit, production, contracts, anticipated profits, revenues, anticipated savings, operation time, goodwill, reputation or business opportunity, or for any indirect incidental, punitive or consequential loss or damage.
```

4.4.2 Cloud-computing issues with that approach
Certain heads of loss which are often excluded by a supplier in an IT outsourcing 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 of a customer if there are service issues\(^8\).

- 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\(^9\). 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. However, typical clauses will remove any opportunity to recover these types of losses where the supplier is in breach. 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 customers need to be prepared to consider carrying or mitigate in another way, for example by implementing an appropriate disaster recovery solution – the cost of which will impact the business case for choosing a cloud service.

4.5 Confidentiality

4.5.1 The IT outsourcing approach
Confidentiality is good example of a clause often treated as almost ‘boilerplate’ in an IT outsourcing agreement which might not work when included within 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.:

```
12.2 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; or
```

4.5.2 Cloud-computing issues with that approach
Where data is transmitted via a non-secure network e.g. the internet, there is a growing risk that this could be considered as it being akin to becoming publicly known – at which point certain types of confidentiality clauses would no longer impose a contractual duty of confidence on the data. This issue may turn on the precise drafting of the clause but IT outsourcing agreements need to be closely scrutinised to determine whether such clauses correctly function in a cloud-computing context.

4.6 Service levels

4.6.1 The IT outsourcing approach
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. The customer will look for an overall ‘end-to-end’ service level, often this will include an “Availability” measure targeting the level which the customer expects the service being contracted for to be available to them.

4.6.2 Cloud-computing issues with that approach
Where service provision is entirely over the internet, any service level that measures the availability of a service is
dependent on internet performance for the measurement of the ‘end-to-end’ service availability. The last three years have seen numerous high profile examples where internet availability has been affected by factors no supplier of cloud service would take responsibility for, for example:

- political unrest\(^{10}\);
- denial or service attacks\(^{11}\); or
- accidents cutting submarine telecommunication cables\(^{12}\);

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 very recently there are examples of large providers looking to provide 99.9% uptime SLAs\(^{13}\).

4.7. Audit

4.7.1. The IT outsourcing approach

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. If you work in regulated sectors such as financial services\(^{14}\) or public sector procurement\(^{15}\) it may become a legal/regulatory requirement. The explicit contractual right to access and audit property/data is captured in a contract clause e.g.:

```
Audits
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.
```

4.7.2. Cloud-computing issues with that approach

It is likely that a cloud-provider will find it:

- difficult if not impossible to identify the exact physical location of individual service provision or data storage locations for an individual customer; and
- impossible to allow one customer access to service provision locations without opening itself up to accusation of

4.8. Termination/exit

4.8.1. The IT outsourcing approach

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:

```
1.2 The Deliverables in relation to the Exit Plan shall include:
(a) relevant available information about proprietary products, tools and methods and the access to information to be provide by the Service Provider to the and/or a Replacement Service Provider;
```

4.8.2. Cloud-computing issues with that approach

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 – is 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. Customer should therefore look to agree with suppliers prior to contract signature a detailed exit plan which will include:

- 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;
- detail 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?; and
- timescales for the transfer of the customer’s data.

---

\(^{10}\) http://www.bbc.co.uk/news/technology-12306041.

\(^{11}\) http://news.bbc.co.uk/1/hi/technology/7228315.stm.

\(^{12}\) http://www.bbc.co.uk/1/hi/technology/11980125.


\(^{15}\) OGC Model Terms and Conditions of Contracts for Services – http://www.ogc.gov.uk/Model_terms_and_conditions_for_goods_and_services.asp.
4.9. Policies/standards/security?

4.9.1. The IT outsourcing approach
Whilst an outsourcing customer wishes to outsource a business function, such a customer will also want to ensure 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.:

4.9.2. Cloud-computing issues with that approach
Simply 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 customers being supported from similar delivery centres or, if they can be complied with, will be at significant extra costs. That is why, suppliers will often offer customers a contractual promise to meet standards and policies but they will be the suppliers standards and policies which the customer will have to consider if they meet their own requirements.

5. Conclusion

The then UK Government CIO John Suffolk said at the Parliamentary IT Committee in January 2010 that security and data protection and privacy are key concerns in cloud computing and “...We have to know every bit of where everything is – hard in the old world, even harder in a cloud world. But we are in a position where the money has run out. So do I think cloud is right for both public and private sector? Absolutely so. And will we do it? Absolutely...”16. Therein lies the issue. Private and public sector customers need the efficiencies and cost savings that cloud-computing can bring regardless of the operational and legal risks that can be identified. This is going to put a demand on the agreements that allocate the risks and rewards of cloud computing between customers and suppliers. What seems clear is that whilst the technology might be undergoing evolutionary development, the contracts that govern them might need to be revised in a more revolutionary way to adapt to the new delivery method.

Andrew Joint (Partner) (Andrew.Joint@kemplittle.com)
Edwin Baker (Solicitor) (Edwin.Baker@kemplittle.com) Commercial Technology Team, Kemp Little LLP UK