Cloud Computing

A buyers guide

KEMP LITTLE

KEMP LITTLE

Contents

Introduction

In the traditional computing infrastructure, a computer's operating system (e.g. Windows), applications (e.g. Microsoft Word) and data (e.g. documents) are typically stored on an individual user's computer. In the office environment data is usually stored on servers (often within the same building) which are then universally accessible by the rest of an organisation.

Cloud-computing is a different form of IT infrastructure. Information, software or other IT services are stored and accessed via third party servers connected to the Internet, rather than on individual computers or on private servers. This is not a new concept. Anyone who has a web-based email account such as Hotmail or Gmail, is using a simple form of cloud-computing.

In 2008 Merrill Lynch estimated that by 2011 the global market for these cloud services[1] would have a value of around US$160 billion. By 2009 Gartner estimated that the global market had a value of around $46 billion with a predicted rise to around US$150 billion[2] by 2013.[3]

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] 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.
[2] The Cloud Wars: $100+ Billion at Stake, Published by Merrill Lynch, 7 May 2008.
[3] http://www.gartner.com/DisplayDocument?id=914826.

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

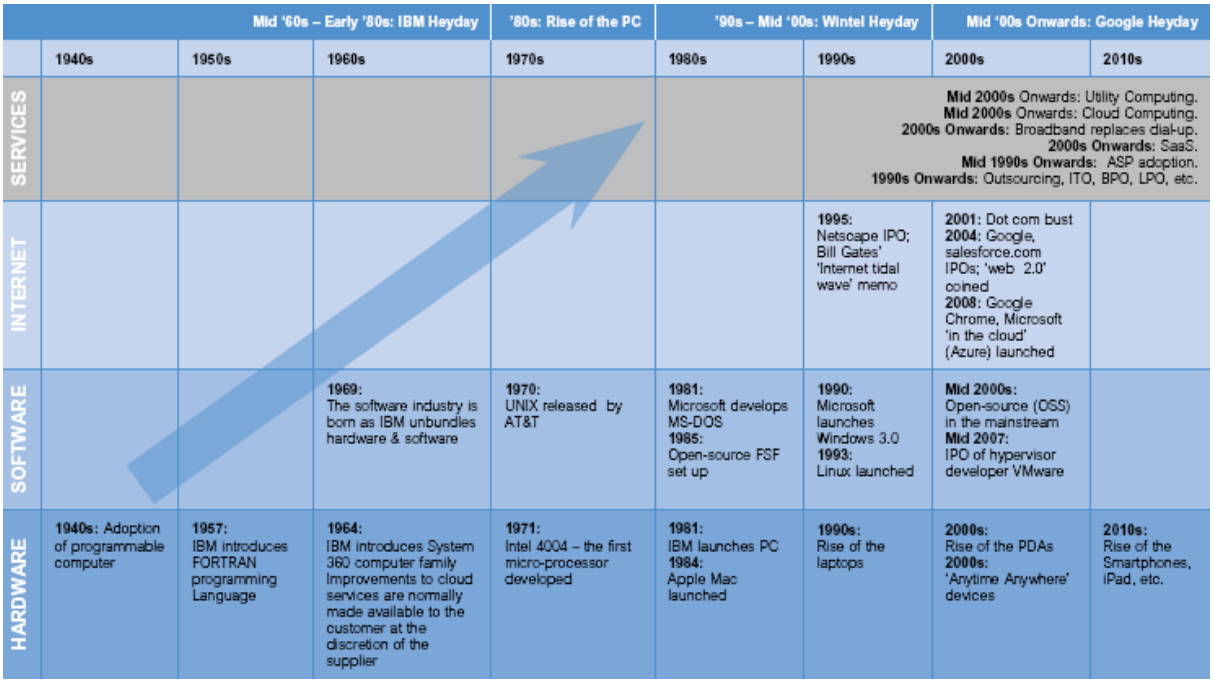
“Prediction is very difficult, especially about the future...”[4]

Figure 1 The rise of service based computing

The current cloud solutions being offered by IT suppliers are the latest evolutionary step in the delivery of IT which has progressed over the last 50 years.

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

- hardware developments from the 1940s;
- software developments of 1969 onwards; and
- essentially for the “cloud", the rise of the Internet.



Cloud-computing services form part of the service based computing trend and we focus on this in this section describing IT outsourcings, 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.

[4] A quote often attributed to the Danish Physicist Niels Bohr.

1.1 Early IT outsourcings

IT outsourcing is perhaps the most iconic and best 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, maintain, support and update the customer's desktop computers.

The key advantages 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 effectively run the outsourced function. The customer therefore avoids needing to employ a number of IT specialists as 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 should be satisfied for either a set charge or 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 "peaks and troughs" involved in the costs for refreshing IT hardware/software.
- Potentially avoiding the locking up of capital in infrastructure. Often the IT supplier will own the IT 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.

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.

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.
- It allows for customised and "bespoke" 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.
- 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.

1.3 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 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.

1.4 Common Types of cloud-computing

The most common types of computing services that are widely talked about as “cloud-computing” are:

1.4.1 Software as a Service (“SaaS”)

As described in section 1.3.

1.4.2 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”.

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”).

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.

1.4.3 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.

1.4.4 Everything as a Service ("EaaS" or "XaaS")

This is a hybrid term referring to a combination of SaaS, IaaS and PaaS.

1.4.5 Utility Computing

Utility computing is not really a development past cloud-computing, more a refinement of EaaS 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 metered basis, like electricity or another utility.

Instead of a SaaS arrangement where a customer will look to access a specific piece of software over the Internet, in Utility Computing the customer is looking to access computing power to meet a requirement e.g. email, store data etc., and the supplier is able to meet the requirement however (and in the most cost-effective way) they like.

The advantages of Utility Computing are:

- that it claims all the benefits of "cloud" and SaaS but is customer requirements driven; 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.

2 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 IT outsourcing contracts to be used for cloud based services is not necessarily a useful approach. In legal terms a revolution in contract clauses, a large upheaval from traditional IT contract precedents, is far more realistic for some clauses.

However, a customer that switches from using IT infrastructure on site 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-sourcing 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;
- it 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 to which 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 Outsourcing depending on whether this involves offshoring/onshoring); and
- are typically embodied in a contractual structure which contains a significant level of detail.

As there is significant overlap between the scope of IT outsourcings and cloud-sourcing 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-sourcing 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 that are 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 delivery 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 or 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 cloudsourcing deal will not typically involve the transfer of assets and staff or typically 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 cloudsourcing payment models are typically much simpler to calculate and may be charged on a "pay per use" basis. While the cloud-sourcing calculations may 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 so ascertain the extent of the cost saving which is meant to 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 typically made available to the customer at the discretion of the supplier as and when these are developed. A cloud-sourcing has less scope therefore for agreeing future functionality by a pre-defined stage in the contract.

- IT outsourcing deals are typically longer, more complex, and higher value. Cloud-sourcing deals, on the other hand, are typically for shorter terms, less complex and for lower values. While this is slowly changing as the market for cloud services matures, this lower value and shorter term limits the degree to which suppliers may be prepared to negotiate highly customised contractual terms for a cloud-sourcing deal.

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

DIFFERENCES BETWEEN IT OUTSOURCINGS AND CLOUD SERVICES

Key differences	IT outsourcings	Cloud services
Customisation	Typically a highly customised service tailored to the customer's requirements	Typically a uniform solution on the basis of a one-to-many model
Delivery of services	The supplier is responsible for delivery of the services	Customer is more concerned with availability rather than delivery
Pricing	Pricing payment models can be extremely varied and typically complex	Payment models are usually much simpler to calculate and may be charged on a pay-per-use basis
Upgrades and improvements	Often involve provisions that seek to improve the services over the term of the contract	Improvements to cloud services are normally made available to the customer at the discretion of the supplier
Length	Typically long, complex and high value	Tend to be for shorter terms, less complex and for lower values, which limits the degree to which suppliers may be prepared to negotiate a customised contract

3 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 cloudsourcing arrangements. Those are:

- the Data Protection Act 1998; and
- MiFID/SYSC rules (where relevant).

3.1 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 cloudsourcing 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 cloudsourcing arrangements will need to ensure that their agreements with their cloud-sourcing provider comply with their obligations under the DPA and Principles.

The key Principles which will have an impact on a cloudsourcing are:

3.1.1 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 personal data. Consent can generally only be given when an individual has been provided with sufficient information to make an informed decision.

Cloud-sourcing issue: Providers typically store and process data on numerous servers at a myriad of locations as this can be the most technically efficient and lowest risk method of storing large volumes of data (and so keeping costs low). Can consent actually be given due to the lack of certainty or understanding as to how the data is to be processed and where it is being sent?

3.1.2 Seventh Principle

Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing or accidental loss or destruction of personal data.

The Principle enshrines the concept that the standard of protections for personal data will be implemented according to the type of information, the cost of implementing solutions and the potential damage which would be caused by its loss.

Cloud-computing issue: It is likely that in almost all cloudsourcings, 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.

3.1.3 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.

3.2 MiFID/SYSC rules

Where a business is regulated by the Financial Conduct Authority ("**FCA**") and/or the Prudential Regulation Authority ("**PRA**") in the UK then that business will need to be wary of specific rules imposed by the FSA.

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 then that

[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.

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 FSA 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 cloudsourcing an attractive option.

3.3 Proposed Network and Information Security Directive

On 7 February 2013, the European commission and High representative of the EU for Foreign Affairs and Security Policy adopted a Joint Communication, labelled *'Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace.'* [10] Additionally, a proposal for a Directive of the European Parliament and of the Council in relation to requirements for a high common level of network and information security across the EU was also adopted[11], along with an executive summary[12] and impact assessment.[13]

This has been labelled the 'Network and Information Security Directive', but is also commonly referred to as the 'Cyber Security Directive'. In March 2014 the European Parliament voted to adopt an amended version of the Directive[14], although this has yet to be adopted by the Council of Ministers. The proposed directive is currently

[7] SYSC Rule 8.1.8(10).
[8] SYSC Rule 8.1.8(7).
[9] SYSC Rule 8.1.8(9).
[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF
[11] http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf
[12] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1668
[13] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1669
[14] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN&language=EN

going through the ordinary legislative procedure, as various European institutions publish their Opinions on the proposal and its likely impact.

The Directive forms part of the overall Cyber Security Strategy of the EU, which articulates the following five strategic priorities:[15]

- Achieving cyber resilience;
- Drastically reducing cybercrime;
- Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- Developing the industrial and technological resources for cyber-security;
- Establishing a coherent international cyberspace policy for the EU and promote core EU values.

The proposed Network Information Security (NIS) Directive will include provisions covering the following areas:

- National Frameworks on Network and Information Security. Essentially, Member States will need to adopt a NIS strategy and appoint a national NIS authority with sufficient resources, both human and financial, to prevent, handle and respond to NIS risks and incidents.
- Co-operation between Competent Authorities: A mechanism will be introduced to assist co-operation between member states and the Commission in relation to sharing early warning signs of emerging risks and incidents.
- Security of the networks and information systems of public administrators and market operators: The operators of critical infrastructures in certain sectors, (e.g. health, transport and energy), along with the enablers of information society services (e.g. app stores, e-commerce platforms, cloud-computing providers, social networks, search engines and digital payment systems), along with public administrations, would need to adopt risk management practices and report major security incidents on their core services.

Cloud-computing issue:

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 cyber-security legislation will undoubtedly have knock-on effects for service providers and users in the cloud-computing sphere.

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF

3.4 European Commission SLA guidelines

In June 2014, the European Commission published guidelines relating to service level agreements (SLAs) for cloud services.[16] SLA terminology often differs dramatically from one service provider to another, thus it can be difficult for cloud service customers to compare cloud services.

It has been argued that standardising aspects of cloud SLAs will improve clarity and understanding of cloud concepts and services within the market. Therefore, the European Commission's Cloud Computing Strategy[17] has called for the development of standardised terms. The published guidelines state that the initiative will have maximum impact if standardisation of cloud SLAs is done at international level, rather than national or regional levels. In particular, international standards, such as ISO/IEC 19086 have been suggested as a good mechanism for achieving this objective. Consequently, the C-SIG SLA Subgroup, which is the European Commissions' expert group on the topic, is to liaise with ISO Cloud Computing Working Group[18] to collaborate and articulate a European position. Going forward, the SLA Guidelines are to serve as a basis for further work of the C-CIG SLA and further contributions to the ISO/IEC 19086 project.

In October 2014, the aforementioned cloud SLA guidelines were passed on to the International Organisation for Standardisation (ISO) working group on cloud computing.

Cloud-computing issue:

The cloud SLA guidelines are designed to reassure cloud customers that contracts with cloud providers will meet certain key requirements, which include the following:[19]

- the availability and reliability of the cloud service being purchased
- the quality of support services they receive from their cloud provider
- what happens to their data when they terminate their contract
- the security levels they need for their data
- how to better manage the data they keep in the cloud.

Stakeholders will need to stay alert to developments in this area, in relation to both SLA terms and international standardisation certifications.

[16] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[17] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[18] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=601355
[19] http://ec.europa.eu/digital-agenda/en/news/standardised-cloud-service-contracts-step-closer

4 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:

4.1 Service Performance

The IT Outsourcing Approach

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, customer's 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."

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 "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 market-place.

4.2 Compliance with Applicable Laws

The IT Outsourcing Approach

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).

Cloud-computing issues with that Approach:

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.

4.3 Limits on Liability

The IT Outsourcing Approach

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 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;"

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 to offer multiples of charges of limits on their liability as the risk doesn't match the reward.

4.4 Exclusion of Losses

The IT Outsourcing Approach

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 savings, operation time, goodwill, reputation or business opportunity, or for any indirect incidental, punitive or consequential loss or damage."

Cloud-computing issues with that Approach:

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.[20] Use of new service offerings by a customer, especially one where security and integrity issues are publically 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 agreement, 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.

4.5 Confidentiality

The IT Outsourcing Approach

Confidentiality is 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."

Cloud-computing issues with that Approach:

Where data is transmitted via a non-secure network e.g. the Internet, this could be considered as being akin to it becoming publically 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.

[20] http://news.bbc.co.uk/1/hi/technology/8303952.stm

4.6 Service Levels

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. Often the customer will look for an overall "end- to-end" service level, often this will include "Availability" measures targeting the level at which the customer expects the service being contracted for to be available.

Cloud-computing issues with that Approach:

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" service availability. The last six 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;[21] or
- accidents cutting submarine telecommunication cables.[22]

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.[23]

4.7 Audit

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, or if you work in regulated sectors such as financial services[24] or public sector procurement[25] 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.:

"XXXX may, not more than once in any contract year in respect of each of the following, conduct audits for the following purposes:

[21] http://www.bbc.co.uk/news/technology-12306041.
[22] http://news.bbc.co.uk/1/hi/technology/7228315.stm.
[23] http://www.informationweek.com/news/infrastructure/management/showArticle.jhtml?articleID=229100165&cid=RSSfeed_IWK_All.
[24] Senior Management Arrangements, Systems and Controls - SYSC Rule 8.1.8 - http://fsahandbook.info/FSA/html/handbook/SYSC/8/1.
[25] OGC Model Terms and Conditions of Contracts for Services - http://www.ogc.gov.uk/Model_terms_and_conditions_for_goods_and_services.asp.

(a) to verify the accuracy of charges

(b) to review the integrity, confidentiality and security of the XXXX data."

Cloud-computing issues with that Approach:

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 locations without opening itself up to accusation of security and confidentiality breaches to their other customers.

4.8 Termination/Exit

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:

"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."

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 – 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 will 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 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.

4.9 Policies/Standards/Security

The IT Outsourcing Approach

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.:

"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."

Cloud-computing issues with that Approach:

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 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.

5 Conclusion

The then UK Government CIO John Suffolk said at the Parliamentary IT Committee in January 2010 that security, data protection and privacy are key concerns in cloud-computing.

"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."[26]

And therein lie the issues. 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.

"Do I think cloud is right for both public and private sector? Absolutely so."

John Suffolk – UK Government CIO – January 2010.

Andrew Joint, Partner, Kemp Little LLP

This guide provides a clear and user-friendly introduction to the concept of cloud-computing, by contracting 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.

02.2015

[26] http://www.pitcom.org.uk/modules.php?op=modload&name=News&file=article&sid=214&mode=thread&order=0&thold=0