

BIRD & BIRD

Bird & Bird
Technology Knowledge Group

CLOUD COMPUTING

Roger Bickerstaff
Barry Jennings

20 November 2009

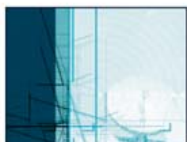


Table of Contents

Page 1

Introduction	2
What is Cloud Computing?	3
The Benefits & Risks of Cloud Computing	4
Cloud Computing & Outsourcing	6
The Monetisation of Cloud Computing	8
Contractual Issues	10
Service Levels	15
Service Credits	18
Jurisdiction & Governing Law	20
Compliance Issues	23
Cloud Computing Checklist	27
About the Authors	28



Cloud computing is a rapidly growing trend in IT sourcing that, along with Web 2.0 operators, social networking sites and software virtualisation technologies, is driving the continuing development of the web as the key IT platform in the early twenty-first century.

At its most basic, cloud computing is the delivery of IT as services via the internet. The big idea is that users will no longer need to purchase or install software and companies won't run their own application and data servers. Cloud service providers will host applications and provide the computing power from their data centres – benefiting from massive economies of scale and dramatically lowering the costs of IT.

Cloud computing is not new though. Cloud computing is a development from the Application Service Provider (ASP) model that was much hyped towards the end of the last millennium and Salesforce.com has been offering its CRM software from the cloud since 1998. To many, cloud services are akin to older models such as mainframes and bureau services. However, there is much speculation within the IT industry and the online media that we are fast approaching the tipping point for cloud computing. Increased reliability of the internet plus the development of more sophisticated encryption technologies mean companies are able to look more seriously at cloud computing based offerings, attracted by the apparent cost benefits. The continuing recession and its impact on IT budgets means that almost all companies and public sector bodies need to at least explore cloud computing as an option for their IT provisioning.

Cloud computing based arrangements are usually paid for on a service basis, which means that the upfront costs and upgrade fees associated with more traditional software licensing should be avoided (running a virtual machine on Amazon's Elastic Computing Cloud (EC2) starts at just ten cents per hour). However, this is by no means always the model adopted, and some cloud computing service providers may seek to levy start-up fees or upfront subscription charges to mitigate their own commercial exposure, for example, for any third party software licensing charges.

The nature of cloud computing based arrangements means that a number of well-established IT contract concepts need to be reconsidered. Furthermore, the increased regulation of business through data protection, Sarbanes-Oxley and MiFiD provides a challenge for organisations looking to move to web-based software and data storage. This paper looks at the nature of cloud computing arrangements and examines the key commercial and contractual issues facing customers and suppliers.

There are varying definitions given to the “Cloud” and for cloud computing – often depending on which company or consultancy you speak to. This reflects the vast array of different services that are available and the different business models that companies are adopting. That said, it is generally accepted that cloud computing consists of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) – all of which involve delivering IT components that had previously been regarded as products or tangibles (transactions) in a different way (relationships).

Software as a Service

Software as a Service (SaaS) is the delivery of a service by an IT provider that remotely hosts and manages software applications (for example, e-mail, word processing, CRM, spreadsheets) for its customers and provides initial and ongoing support services. True cloud computing services follows a "one-to-many" model – there is a standard software product, of which a service provider allows many customers to access the same version. The software is not tailored for specific client requirements although a good SaaS offering allows a degree of configuration to suit individual business needs. Although some SaaS service providers offer customer-specific customisation services, this undermines the cost benefits of a "one-to-many" model. This means SaaS services were initially regarded as being most useful for individuals and SMEs and for the more standardised software applications, like e-mail, word processing, CRM and accounting. However, this is gradually changing as SaaS offerings become more sophisticated and traditional IT companies, like Microsoft, develop hybrid models of Software plus Services (where some locally installed software is still used – to offer richer feature lists than pure SaaS – but where data, content and extended features are accessed online). This is beginning to make cloud computing more attractive to larger enterprises and public sector organisations.

Platform as a Service

Whereas ASPs often licensed software from third parties to host on an ASP basis and offer to their customers, the software vendors themselves have promoted the cloud computing model, going to the customer direct. This is changing, however, with Google and Salesforce both offering Platforms as a Service (PaaS) where third parties can host their software applications in order to distribute them to customers. This allows smaller software vendors to avoid the prohibitive costs of large-scale data centre purchases and provide a channel to customers (see Apple's App Store), so reducing the cost to market for new cloud computing applications (see 'the Monetisation of Cloud Computing' below).

It is not just core IT businesses that are moving into the cloud computing market. Amazon, the online retailer, launched its pioneering Amazon Web Services in 2006, allowing anyone to start a virtual machine on its computer systems to run a web-based service and leveraging the considerable technology expertise it had built up in managing its own sophisticated computing platform.

Infrastructure as a Service

Also known as Hardware as a Service, Infrastructure as a Service concerns the delivery of computing resource - servers, network equipment, memory, CPU, disk space, data centre facilities. These are often shared resources with automated load balancing and resource scaling – capitalising on virtualisation technologies and avoiding the costs of hardware sourcing (and making such investment an operating expense rather than a capital expense).

Cloud computing has attracted considerable commentary from the media and professional services firms, as well as the hype generated by suppliers' own marketing teams. Undoubtedly, cloud computing presents a number of opportunities for individuals and organisations of all shapes and sizes. However, as with all IT and outsourcing arrangements, it is not without risk. The balance of risk and benefit will vary from customer to customer, supplier to supplier and deal to deal but Table 1 below seeks to capture the most commonly recognised features of cloud computing.

Table 1 – The Benefits & Risks of Cloud Computing

Benefits	Risks
Low, fixed periodic service charges	Untailored solutions may not precisely match corporate needs
Improved support & maintenance – the “permanent beta”	Contracting on fixed standard terms
Anytime, anywhere access	Lack of integration and management of legacy systems
Minimises hardware investment costs	Lack of control over data and content
Low barriers to take-up – cloud computing is designed to be user-friendly and minimise specific training requirements	Risk of lock-in – need to escrow source and object code plus data
Support by advertising can further reduce costs	High risk of service provider failure for new services due to high start-up costs and low initial returns
Costs of cloud computing should decrease over time as users increase	Risk of hidden extras for additional users, storage and so on
Reduces internal management overhead	Compliance issues – data protection, encryption, Sarbanes-Oxley, MiFiD
“Elastic” IT – can expand or contract as required	Complexity of contracting and management in multi-sourcing arrangements
Part of the green ICT agenda – organisations can outsource their carbon usage to organisations geared up to manage and minimise that impact	Reliance on online connectivity – the internet is fast becoming a single point of failure for many organisations – how long could a company operate without it?

Cloud computing has had a place within the consumer market for some time now but the majority of larger companies and public sector bodies were much more apprehensive. These attitudes are changing and cloud computing is an option for almost all organisations (even if still eventually dismissed). Table 2 below seeks to reflect this shift in attitudes among market groups from red towards green and highlight the features of cloud computing that are most attractive to the different groups.

Table 2 – Attitudes towards Cloud Computing

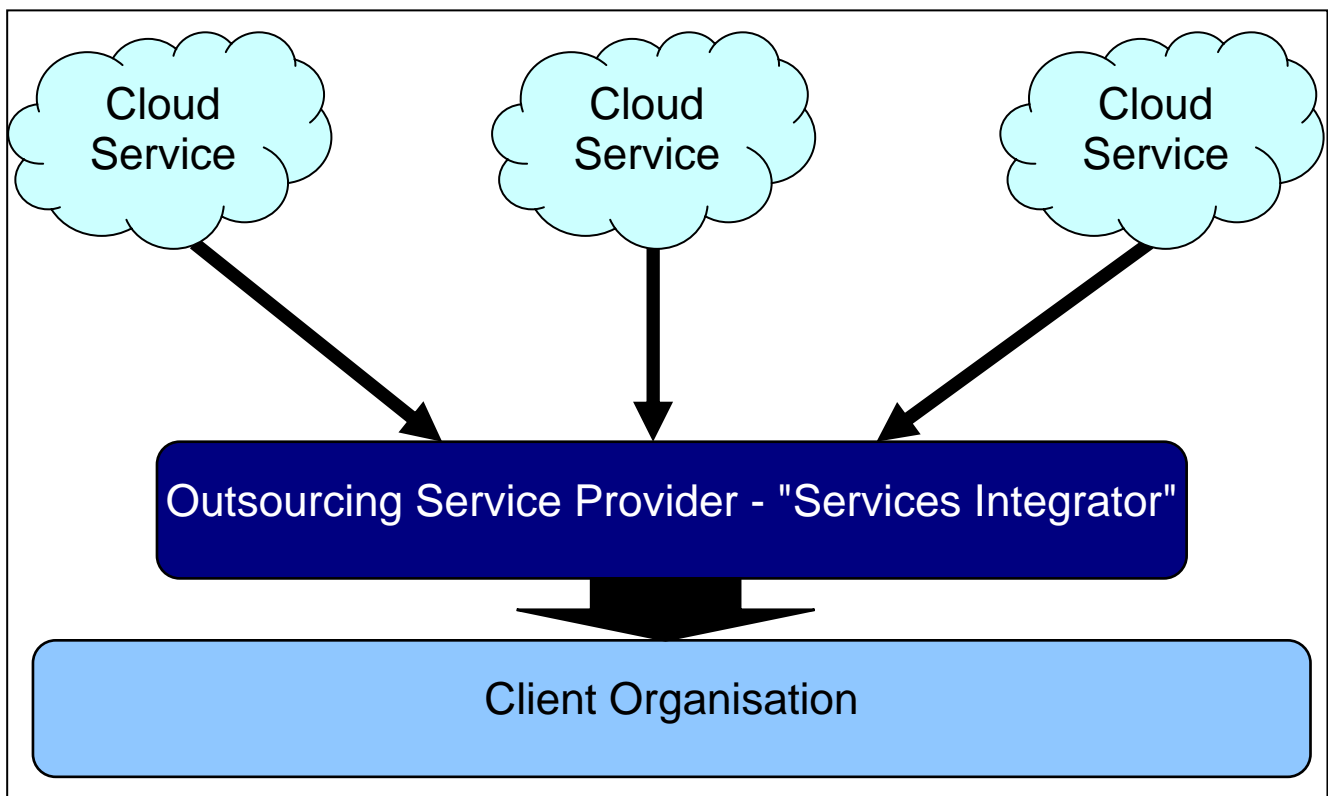
Consumers	Mature market – low or no cost (funded by advertising) Flexibility of access at home, work & on the move
Start-ups	Removes barriers to entry (cost) & growth (difficulty in scaling) that needing a sophisticated IT infrastructure had previously posed
SMEs	Empowers employees – flexibility & innovation Predictable costs – OpEx not CapEx
Large Corporates	Re-balancing of risk profiles – re-assessing what needs to be controlled Use private clouds or restricted-use clouds to get some of the benefits
Multinationals	Flexibility in global deployment – increase market responsiveness
Public Sector	No longer red due to cost-cutting imperative Public sector clouds & shared services programmes

Cloud computing arrangements differ from traditional outsourcing and facilities management arrangements, both in respect of the type of service provided and the ownership of the assets used to provide the service. However, customers and suppliers are increasingly seeing cloud computing as one of the toolsets available for outsourcing of IT.

Some organisations are using cloud computing as one element of multi-sourcing arrangements – enabling them to be flexible in choosing IT services that best meet their needs rather than single monolithic outsourcing arrangements. However, other organisations still see value in contracting with a single outsourcing service provider (OSP) who acts as a “Services Integrator” drawing together a number of cloud services (see Figure 1 below) and taking responsibility for ensuring these are integrated with non-cloud IT components and legacy or bespoke systems.

For larger organisations that may not be ready to consider surrendering their data and applications to the public cloud, a number of operators and some in-house teams are realising some of the benefits of cloud computing from establishing private clouds.

Figure 1 – The Services Integrator



The use of cloud computing for outsourcing has a number of aspects that have a significant impact on the customer-supplier relationship. There will be particular features in any deal or arrangement that need to be given careful consideration but the areas highlighted below are common variations with most cloud arrangements.

Customisation

Cloud computing solutions are generally not tailored for individual customers and this has so far meant that most large organisations have continued to use traditional licensing, support and maintenance arrangements, particularly where they see value in the customisation of their software applications. However, cloud computing is a part of the strong trend towards utility computing where business processes and configurations are regarded as being more important for harnessing competitive advantages than the underlying hardware and applications.

Support

Cloud computing service providers can provide expertise in the operation and support of particular software applications and in most cases have control over the operating environment. This means that the level and quality of support should be higher in a cloud computing set-up than in ordinary customer support and maintenance arrangements. Furthermore, most cloud computing systems operate as a "permanent beta", meaning that there are no versions in the traditional sense – as new functionality is added or bugs are fixed, these are incorporated into the online application. This means that the application you access through your web browser is always the most up to date without the need for costly upgrades.

Software

Under a cloud computing arrangement, the software forming the basis of the service will generally be packaged software hosted and maintained by the cloud computing service provider. Under an outsourcing arrangement, however, the OSP will provide services based on a range of applications, both packaged and specially written. The OSP will also often take on the operation, management support and ongoing development of legacy software that the customer may have acquired over many years prior to the commencement of the outsourcing arrangements. Customers need to consider their requirements carefully in this respect and this is where many OSPs see that they can still add significant value in a cloud-based IT world through acting as "Services Integrators".

Hardware

The hardware used to host cloud applications will generally be owned or leased by the cloud service provider. This is also the case in most IT outsourcing arrangements when the OSP owns or leases the hardware. However, in cloud computing arrangements the software is located on the service provider's servers at its premises and is accessed by the customer on a remote basis by means of transmission arrangements between the customer and its internet service provider (ISP). This is different from most traditional outsourcing arrangements where the software tends to run on local devices (such as desktop PCs) on the customer's premises (although increasingly in recent years, virtualisation technologies from organisations such as Citrix, VMWare and Microsoft have allowed OSPs to host software at their own premises).

Exit/transition

One often-overlooked element of cloud computing is the risk of lock-in. The need for exit or transition provisions within IT outsourcing arrangements is well-recognised but with cloud computing there is less clarity at present. For example, if an organisation has to back up all of its data on its own servers to ensure that it will have access to it if it seeks to terminate its cloud computing arrangements then this would negate much of the cost benefit of cloud computing (see Figure 2 below).

Cloud computing contracts are service contracts rather than software licences. Cloud service providers may look for a minimum duration and may offer further discounts to encourage customers to sign up for longer periods in order to secure long-term revenue streams. However, customers should be wary of becoming locked into an arrangement that could cease to meet their changing business needs.

Most cloud service providers forego upfront licence fees for the predictable long-term revenue offered by service payments. SaaS vendors are looking at a "long tail" revenue model where they have a small fee but a large number of customers continuing to use the service for a long time. The low set-up costs to new customers and the ease of deployment via the internet mean that good products have the potential for rapid, exponential growth in customer base (conversely, bad solutions are swiftly dropped by unsatisfied customers). Service providers may also support themselves by allowing advertising on their sites and this can even lead to some cloud computing service providers offering their basic packages free of charge.

Some cloud service providers (particularly smaller start-up operators) may look to pass some initial set-up costs on to a new customer, although this is much less common than under ASP arrangements. There may be an initial "licence fee" payment for the software even though the customer will not actually acquire a "copy" of the software as such.

Some potential cloud service providers looking to act as the intermediaries between developers and customers still struggle to get third parties to license software to them without an initial licence fee as they are unwilling to accept the risk of another organisation's business being successful. The software industry has traditionally sold products rather than services, and licensors can be reluctant to accept service level regimes which outline expected service standards. These sorts of supply chain problems are likely to improve if the new business model proves viable over time but there may also be a competition law angle if dominant developers look to bundle their best software on their own "clouds" or refuse to provide a platform for certain organisations' software.

The cloud service provider may also look to recover some costs associated with the purchase of items such as hardware and transmission links when setting up a new customer. These initial set-up costs undermine the supposed benefits of cloud computing so most service providers look to avoid levying them but this can make the cost and risk of setting up a cloud computing based system prohibitive. This has led larger operators, such as Salesforce, Google, Amazon and Microsoft, to look at offering Platforms as a Service (PaaS) where they provide software developers with the necessary web tools and hardware platform on a rental basis. This reduces the upfront cost of development and deployment of cloud computing solutions and removes the need to require any initial set-up charges from customers.

Periodic & Usage-based Charging

The pricing arrangements for ongoing cloud computing services usually follow one of two models: periodic charging or usage-based charging. Periodic charging is the most common model and usually involves a set subscription fee based on the number of users and an overall or per-user storage limit. This fee may be payable monthly, quarterly or yearly. This offers a degree of certainty and the basic package is often sold cheap, with service providers making most of their profit from "upselling" of add-ons and premium packages.

Usage-based charging relates the charges to be paid to the amount of usage of the service by the customer. This can be attractive to customers, particularly where their policies and practices enable

them to make best use of the service and minimise wasted charges. However, usage arrangements tend to pass the business risk of IT use back to the customer, which makes charging less predictable, so that the customer loses one of the key benefits of cloud computing. This model may also be unattractive to the cloud service provider, since the charges it receives will fluctuate from one charging period to the next on a basis that is beyond its control.

Additional Charges

Whichever charging model is being used, customers should establish at the outset what the service charges will consist of and what will be sold as add-ons or "hidden extras" (see Figure 2 below). Support and maintenance are often provided for an additional charge based on a percentage of the subscription fee – and these percentages vary between service providers. Service providers also vary considerably in respect of their add-on charges for extra users, extra storage, premium maintenance and uptime guarantees, so it can be difficult for customers to evaluate the overall value for money of different solutions.

Whereas list prices for traditional software licences are seen as something of a fantasy with actual prices paid being heavily discounted in practice, this is less apparent with cloud computing offerings where service providers have needed to strip their standard prices significantly in order to overcome market hesitancy. Discounts are more common around add-ons but these should be negotiated up front by customers rather than at the time when they are needed, when an organisation's bargaining power is likely to be reduced.

Price Increases

As many cloud service providers are start-up companies that are not making an immediate commercial return but are keen to obtain market share, deals may initially be priced attractively from the customer's perspective. Even where the customer is negotiating with a more established vendor, the existence of others willing to undercut prices may influence the level of the charges.

The extent to which price increases are controllable becomes a key issue in these circumstances. Where the parties have agreed an advantageous initial price, the customer needs an assurance that this will not escalate inordinately over the term of the contract. Similarly, a customer will not want to find that, where a short-term contract has been agreed, the cloud service provider is only willing to enter into a new contract at the end of the term if the charges are increased significantly.

Longer-term agreements should therefore restrict price increases. Increases can be capped either by reference to a fixed percentage of the charges paid in the preceding year, to an indexation mechanism such as the retail price index (RPI) or to IT specific indices. IT-specific indices generally track remuneration in the IT industry and are therefore likely to outstrip the RPI. In fact, many of the costs associated with cloud computing may decrease over time in line with the cheaper price of hardware. Price restrictions that relate to IT-specific indices may therefore become relatively favourable to the cloud service provider.

For short-term contracts, customers may seek to negotiate options to renew for a single term or further terms. The charges payable during the renewal terms should be capped, although the customer is always entitled in theory to move to a different vendor if the charges escalate excessively.

As successful cloud service providers will have very high numbers of contracts globally, pure cloud operators generally seek to offer their services on standard terms (that are usually published on their websites). These terms tend to be strongly supplier-centric, excluding all but the most limited of warranties and any liability for data loss or corruption or service failure. In particular, several organisations reserve the right to delete customer data for breach of contract, such as non-payment. In the UK, standard terms (and in particular any exclusions or limits of liability) are subject to the Unfair Contract Terms Act 1977 (UCTA) and therefore must be reasonable but it is far safer to seek to negotiate key provisions in advance rather than rely on statutory protection after an issue arises. It is also likely that customers will need to ask for service levels and service credits to be proposed. For outsourcing arrangements utilising cloud services, agreements will still tend to be heavily negotiated and deal in detail with risk and the allocation of responsibilities of both parties – it would not be in either party's interests to govern these sorts of complex long-term relationships on standard terms.

Another point to note is that if an employee signs up to a cloud computing application using a PC at work for a purpose related to their employment, then the company could be bound by the terms of that cloud computing service. If employees input personal data held by their employer into the cloud, there is an associated risk that the company may not be compliant with its obligations under data protection legislation. Similarly, liability may arise for employees entering defamatory or copyright-infringing content into the public areas of many cloud computing services. As such, organisations should consider whether training or guidance is required to instruct employees on the risks of cloud computing.

The global nature of the internet is ahead of the nationalised nature of most law and regulation. This means that it is easy to envisage scenarios where awkward conflicts of law arise (for example, between legislation allowing enforcement agencies in one jurisdiction to seek the release of information and privacy laws in a jurisdiction where the data is stored). These jurisdictional issues are dealt with in more detail later in this paper.

Negotiating Cloud Computing Agreements

Every cloud computing agreement will need to be tailored to fit the particular context it is intended to cover. There are a number of substantial differences between contracting for cloud computing as opposed to more traditional IT products and services (some of which are explored at a high level below). However, in any service agreement the contracting parties will need to consider and deal with 3 R's - Risks, Relationships & Results.

In the context of cloud computing, risk will be apportioned differently to traditional IT arrangements with customers transferring certain risks to their supplier and taking others back in-house. It is important that the contractual documentation supports the intended transfer of risk or the parties can find themselves in disputes in the future or face an unforeseen liability.

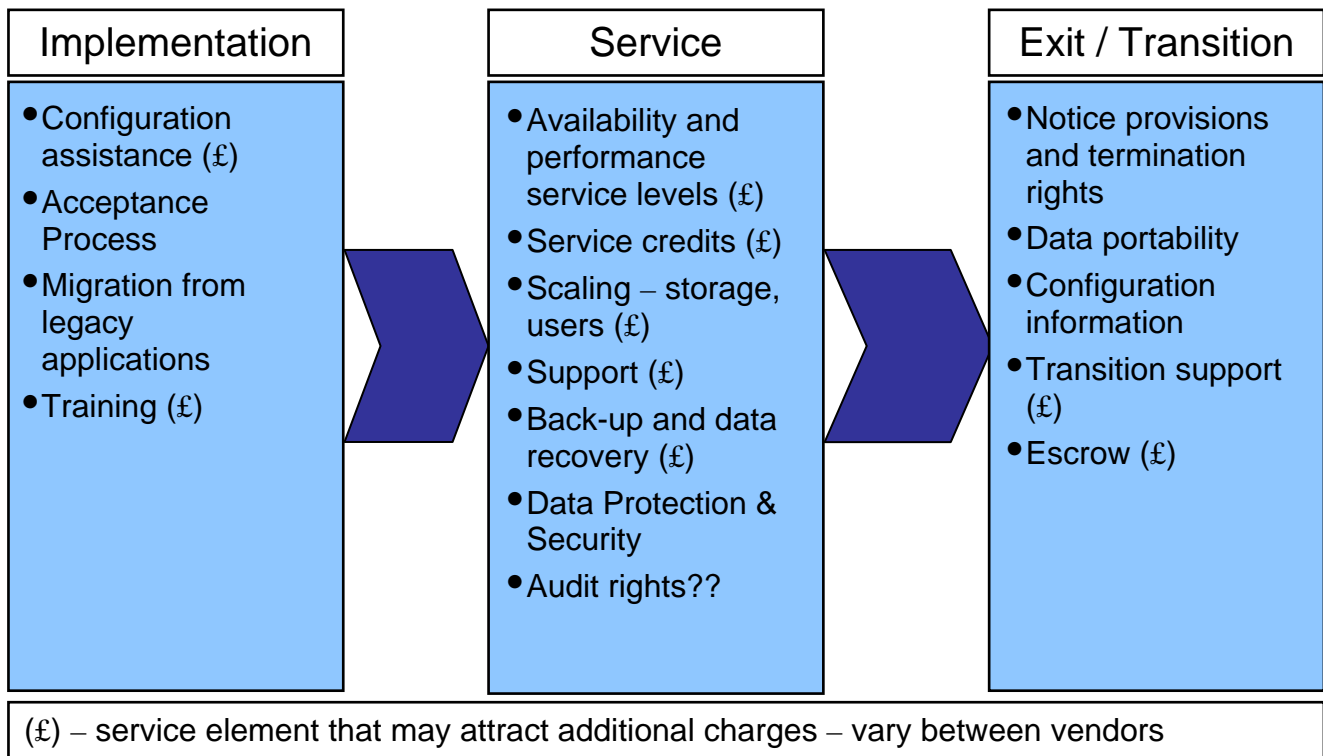
All service agreements need to set the rules for the relationship that will underpin the parties work together. This is just as important for cloud computing arrangements – even if the relationship is conducted entirely at arm's length. How are issues raised and resolved? Who are the individuals on each side that will be responsible for representing their organisations?

Finally, contracting for results is key to making a contract work for both customers and suppliers. Customers want to ensure they are contractually covered for the outcomes they have been promised during the sales process. Suppliers will want to limit results to the realistic and baseline the expectations of both parties. Cloud computing evolved from the consumer space - where failure to

deliver rarely has a significant commercial impact. This is not true of the enterprise market and customers and suppliers need to deal with the implications of non-performance. Service levels and service credits power any service agreement and these are considered in some detail in the following sections of this paper.

When entering into any long-term relationship, both parties should ensure they consider at the outset the entire life-cycle of that relationship – particularly how it might end. Figure 2 provides a high level overview of the points that may need to be contracted for within a cloud computing agreement. This is not a comprehensive list and is focussed on elements that are distinctive within cloud computing arrangements. The diagram also highlights the service areas that are likely to have a charge or cost associated with them (whether broken out with a direct price or included indirectly within the quoted service charge).

Figure 2 – The Contractual & Commercial Issues through the Life of a Cloud Computing Relationship



Cloud computing agreements will vary substantially in reflection of the range of services and approaches that are available. Each agreement needs to be considered in its own context. One thing to note is that simply because cloud computing agreements tend to be lower value it does not mean that they are necessarily lower risk for customers. In fact, the converse may well be true – customers getting lower prices are likely to be taking certain risks back within their organisation that perhaps they are not used to managing (e.g. storage or use limits). This is especially true in multi-sourcing arrangements where customers have to manage multiple supplier relationship. Technical knowledge is not enough – customers need to be highly skilled at project, supplier and contract management to realise the benefits of multi-sourcing and avoid the many pitfalls.

Licensing

Although cloud computing contracts relate to the provision of services rather than to the supply of software to customers, appropriate software licences still need to be granted to the customer. This is because users have online use of software at a PC and, without a licence, this would amount to copyright infringement. These licences are usually very narrowly defined and limited to use of the online application for their own business purposes – customers have no rights to make copies of or modifications or enhancements to the software and they cannot sub-license to third parties.

The cloud service provider will not always own the intellectual property rights (IPR) in the software that is the subject of the cloud computing service. Where this is the case the cloud service provider will need to arrange for the right to sub-license the software to its customers, or for a direct licence to be entered into between the customer and the relevant third party licensor. For the purposes of contractual simplicity, it is preferable (and most common) for the cloud service provider to sub-license the customer's use of the third party software. All of the contractual arrangements will then be between the cloud service provider and the customer. However, software licensors often require a direct licence agreement to be entered into between the customer and the third party licensor. In these circumstances, the cloud computing contract should make it clear that the cloud service provider is responsible for the management of the third party licences, together with the payment of any licence fees. The third party licensor should also be informed that the licence arrangements relate to licensing only. All other issues relating to the provision of the software, such as delivery, installation and configuration requirements, should be dealt with in separate agreements between the customer and the cloud service provider.

Content Licensing

The standard terms and conditions offered by many cloud service providers include a broad licence from the customer to the service provider allowing them to use any content stored on its servers. These licences are often expressed as being perpetual and irrevocable. The uses to which the service provider can put the content are usually limited but there are often rights to pass the content to third parties or use it for the purpose of promoting the cloud computing service. This may not be appropriate for much of the information customers would be looking to store (such as personal data, third party IPR or confidential information contained in or attached to e-mails). Customers should take particular care in identifying any rights they are agreeing to provide to the service provider.

Content Issues

The cloud service provider will look to exclude all liability for content stored or posted on its services and will normally include a right in its standard terms to remove any data from its servers. This is because under the Copyright Directive (2001/29/EC) and The Electronic Commerce Directive (2000/31/EC) internet service providers can be liable for failing to take down offensive, defamatory or IPR-infringing content and cloud computing based applications often blur the line between public and private networks. In such circumstances, corporate customers should seek an indemnity for any loss suffered as a result of material being unnecessarily deleted or moved and should look to impose a requirement to be notified in advance if any content is to be removed.

Shared or Dedicated Infrastructure

The provisions required in the services agreement will depend on whether the platform infrastructure that is adopted will service only one customer organisation (single tenant) or be one that will be shared by a number of organisations (multiple tenant). A shared infrastructure will impact a number of areas including, but not limited to, the termination charge the cloud services provider should seek

to recover on an early termination, the limits it should impose on customer transfer/assignment, the ability customers have to request changes, the breadth of audit provisions a cloud services provider might accept and the indemnities it might be prepared to offer for loss of data.

Business Continuity and Escrow

A comprehensive cloud computing offering will have alternative infrastructures available at a remote location from which the services can be provided in the event of, for example, terrorist bombs, fires, floods and theft. Theft of equipment from the cloud service provider's premises is a particular concern as the equipment is expensive and becoming increasingly portable. Customers may want to negotiate a right to audit and test these facilities, particularly to meet their various compliance obligations (see below). This is likely to be strongly opposed by cloud service providers using shared tenancy infrastructures as such testing might put other customers' data or service availability at risk and service providers will want to avoid multiple audits by multiple customers. This makes it likely that cloud service providers will look to standards compliance and general accreditations or certifications to reassure all of their customers. However, these standards and certifications are currently subject to much debate concerning their merits and adequacy.

From the customer's perspective it is no use including comprehensive contingency arrangements if these will be undermined by the force majeure provision. However, it is impractical to require the cloud computing service provider to carry on providing the services throughout a disaster situation without a measure of relief from the effect of customer remedies.

Customers should confirm what arrangements the cloud service provider has in place in relation to escrow. With cloud computing, customers are putting both their applications and data in the hands of third parties that could withdraw their services at short notice for any number of reasons, so the most reputable cloud service providers usually have "one-to-many" escrow agreements already in place with independent third parties. If the service provider does not have arrangements in place, third parties such as NCC and Iron Mountain are now offering escrow services tailored to cloud computing and SaaS arrangements.

Historically, software escrow has been concerned solely with source code because the object code has been running on the customers' own servers and hardware. This is no longer the case with cloud computing services and it is equally important that the object code continues to be available if the service provider pulls the plug or becomes insolvent as the customer will not ordinarily have it stored locally. In addition, to protect the data inputted into or generated by a cloud application, customers can either back up the data themselves or use a third party online archiving service. Such arrangements provide important protection but add to the overall cost of cloud computing deployment and customers should bear in mind that they will not provide instant service restoration.

IPR Indemnities

It is standard practice in all IT contracts to include an IPR indemnity for the customer's benefit in the event that a third party makes a claim that the use of IT products, particularly software, by the customer infringes the third party's IPR. The inclusion of IPR indemnities in cloud computing contracts is important, because customers have to rely on the cloud service provider to ensure that software licensing issues have been resolved so as to entitle the customer to use the software as part of the service. One of the benefits of cloud computing arrangements is that the burden of the upkeep of software licensing arrangements is generally lifted from the customer. However, if the

arrangements are not properly made, the customer may still infringe the IPR of a third party even though it may have no knowledge of the infringement.

Cloud computing users need to be aware of the possibility of patent infringement through the use of cloud computing arrangements. Patent protection is increasingly available for computer software in the US and, to a lesser extent, in the EU. Where cloud computing arrangements are established on an international basis, the IPR indemnity needs to be sufficiently broad to protect the cloud services' customers in all jurisdictions in which the software will be used.

The performance and quality of cloud computing services are primarily monitored by service level and service credit mechanisms. Service levels provide objective and measurable assessments of key elements of the service. As a result, they are probably the most important part of the cloud computing contract, although they are not always included within cloud service providers' standard terms.

Service credits provide a financial mechanism for customers to put pressure on cloud computing service providers to ensure that the services meet the service levels (see the next section for more detail on service credits). In a software licensing arrangement the customer can make a technical assessment of the software to be provided and decide whether or not the software meets the customer's needs. By contrast, in a cloud computing arrangement (as in IT outsourcing arrangements) the customer is completely reliant on the contractual services descriptions which form the basis of the service to be provided to the customer. Negotiating adequate service level and service credit arrangements is therefore particularly important in cloud computing based arrangements.

Service Availability

Service availability service levels seek to measure the extent to which the cloud computing service is available to users as a percentage of the time during which the cloud computing service provider is contracted to provide the service to the customer. There are a number of issues that need to be considered when negotiating service availability service levels for cloud computing service arrangements, including:

Point of Measurement

Service availability can be measured at a variety of points: for example, measurement can be at the cloud service provider's servers that host the application, at the cloud termination point (where the link is made between the cloud service and the customers' IT infrastructure) or at the end-users' PCs. Cloud service providers normally aim to establish the point of measurement at their servers but this argument should not be accepted without question by the customer. Where the transmission is via the internet there are many different types of internet service provision and the cloud service provider should not be allowed to adopt a potentially low-quality and low-cost approach, with the inevitable impact on service quality, unless the customer understands the approach and has agreed to it.

From the user's perspective, service availability measurement at the user's PC is attractive because the measurement assesses the extent to which the cloud computing service is available to the user. However, this may not be possible if there is no technological method of assessing service availability at the user's PC. A customer needs to have a reasonably sophisticated systems infrastructure to make the measurement but the necessary tools are no longer uncommon.

A cloud service provider can be expected to argue that the service availability measurement at the user PC level is inappropriate as this will introduce downtime (when the service is not available) resulting from the customers' infrastructure failure, rather than from the failure of the cloud service. The service provider may therefore suggest that the point of measurement should be the cloud termination point at the customer's premises. However, if service availability is measured at this point, it will be more difficult for the customer to assess service availability at an individual user level rather than at the aggregate level relating to all of the users to whom the service is provided.

In general terms, where the customer has an important business requirement for the cloud computing arrangement it should carefully consider the advantages of a leased line linkage to the cloud service provider. This will be more reliable and it will be much easier to argue that the service provider should provide "end-to-end" service levels, including the transmission elements.

Service Measurement Period (SMP)

The period when service availability service levels will be assessed needs to be specified, because the choice of the SMP has an impact on the calculation of service level assessment. Whilst a 24-7 service might appear to be attractive (particularly for global organisations), in practice this can lead to there needing to be considerable downtime required before service credits are incurred. For example, a 98% service level would mean nearly 15 hours of downtime in a 31-day month before it was failed, whereas on an 8.00 am to 6.00 pm weekday service around four hours of downtime might be sufficient to trigger service credits. Customers should consider the impact that taking either approach would have on their operations. Downtime that does occur out of hours can be more difficult to rectify quickly as engineers are less likely to be available. With the focus of cloud computing on flexible anytime, anywhere access, out of hours downtime can soon have a detrimental effect on a service that would otherwise have met its service availability targets and which in all other respects is acceptable.

Application Availability

At its most basic, a cloud service provider may provide a "bundled" cloud service comprising, for example, e-mail, internet browsing and office applications (such as word processing and presentations applications). The service availability service level therefore should relate not just to the overall cloud computing service availability, but also to the availability of the individual software applications.

System Response Times

As well as being made available to users, computer systems need to have a prompt response to user inputs. The key measurement of responsiveness is the speed at which the screen responds to user inputs. System responsiveness measures are more difficult to specify in cloud computing contracts than service availability service levels. This is partly because the complexity of the request that the service will be measured against can be highly variable: for example, a complicated data matching and retrieval operation will inevitably take longer than simply inputting data. However, apparently simple operations, such as printing and saving documents, may be relatively complex in a cloud computing arrangement and take a long time. Print processing may require activities by the cloud service provider at the server level that may increase the transmission time taken to activate the printer. For example, when an Australian based user wants to print from a web page provided by a UK based cloud service provider, the web browser servers in the UK have to be activated in order to transmit a print instruction to the user's printer in Australia.

Equally important from the users' perspective are cloud computing helpdesk response times. In particular, will the initial response involve providing answers and user support, or will it simply log the answer with a further call back to provide substantive support? A service provider is likely to use a call logging system as it enables the service provider to meet the helpdesk response time requirement more easily and the personnel for the phones will be less expensive than where fuller user support is provided. It can be useful to include a specific service level for the number of calls

that will be resolved on a "first call" basis to avoid a call logging approach. It is reasonable to expect at least 60% of helpdesk calls to be resolved on a first call basis. Different measures will be required if support is provided only via e-mail.

Additional Hardware

Service levels may not be achieved if any hardware and other equipment used to access the cloud computing service (particularly the transmission elements) has insufficient capacity. Cloud computing contracts usually specify that the customer is responsible for the purchase of additional equipment but customers should look to agree a minimum infrastructure specification that the service provider warrants will be fit for purpose.

Where the cloud computing contract results from a competitive tendering process there is a risk of an "underbid" situation. It is in the bidders' interest to propose a hardware set-up that is the absolute minimum required to keep costs down and win the business. The probity of the bidding process would be put in doubt if a customer were to accept subsequently an argument from the successful cloud computing service provider that the customer should invest in the installation of additional or higher-capacity equipment.

Service credits are the primary financial remedy for a cloud service provider's failure to meet service levels. A series of tables which specify the service credits payable as a percentage of the monthly charges for different levels of failure to meet the service levels should normally be incorporated into the cloud computing contract. Legal considerations include:

Nature of Service Credits

It is a matter of debate as to whether or not service credits in cloud computing contracts are a form of liquidated damages, or a contractual mechanism that sets out the different charges payable by the customer for different levels of service. If the service credits are a contractual mechanism, there are no constraints on the level of the service credits that can be agreed; it is a matter for negotiation between the customer and the cloud service provider. If the service credits are liquidated damages, they should be a reasonable pre-estimate of the customer's likely losses resulting from the cloud service provider's failure to meet the service levels, otherwise they will represent an unenforceable penalty. However, this is a difficult assessment to make. In general terms, the parties should ensure that the level of service credits is not punitive. As an aid to clarity, it may be advisable to include a reference to "liquidated damages" within the clause giving effect to service credits. However, as the courts will look beyond the use of such description (to determine the true nature of the mechanism), it may help the cloud service customer's argument if, prior to entering into the contract, it had considered and documented likely losses from poor service performance.

Customers should be made aware that if service credits are not expressed as liquidated damages in the cloud computing contract, the service provider will not be in breach of contract if it fails to achieve the target service levels. If service credit regimes are not expressed as liquidated damages, they are seen as a contractual mechanism for adjusting prices for varying levels of performance. In contractual terms failure to meet a service level is not in itself a breach because the parties have agreed that a lower price applies for that lower level of service. If the supplier refused or failed to pay service credits associated with a failure to meet service levels, then that would be a breach (with damages being the value of the applicable service credits plus any interest for late payment).

This poses issues in practice when a supplier is commercially better off incurring small monthly service credits rather than pay to fix whatever issue is preventing them meeting the service level. Therefore, customers should usually seek to include provisions in contracts to the effect that the supplier shall (a) put all reasonable endeavours into meeting a service level within [x] months of any failure to meet that service level and (b) provide a rectification plan for agreement by the customer whenever it fails to meet a service level. Failure to comply with these provisions would then be a breach.

Service credits are usually capped at a certain point beyond which the injured party has to claim ordinary damages. This protects the supplier but also the customer (as service credits rarely provide sufficient recompense for major outages or significant service level failures, the cap allows the customer to claim higher damages beyond that point). Customers should usually ask for termination thresholds associated with service levels (a) when performance drops below a certain defined point in any measurement period, (b) when a certain value of service credits have become payable in any [year] or (c) when a service level is not met for [6] consecutive measurement periods. All of these measures fit into the rationale for SLAs which is certainty for both sides and pre-determination of remedies - cutting down some of the scope for future dispute.

It is also worth bearing in mind that a failure to meet a service level is caused by some failure in the services which is often a breach of some specific provision within the requirements/service description/technical documentation. There will, however, normally be a clause limiting recovery of damages where service credits are applicable in order to protect the supplier against double-recovery.

If the service credits are categorised as contractual remedies, the provisions may fall within the Unfair Contract Terms Act 1977 (UCTA). If the cloud computing contract is entered into on the service provider's standard terms, any limitation of customers to service credits as an exclusive remedy must be reasonable (s3(2), UCTA).

Bonuses and Incentives

Service credits are a rather negative means of incentivising the cloud service provider to meet and exceed the target service levels. A more positive financial mechanism is to include bonuses or other financial incentives. Financial incentives and bonuses can be applied on the basis of matrices that are the reverse of service credit tables. The service provider "earns" a bonus depending on the extent to which a target service level, such as service or application availability, is exceeded.

Alternatively, bonuses can be linked to levels of customer satisfaction. This approach is more subjective and is generally based on the users completing satisfaction surveys. However, care needs to be taken to separate out the underlying cloud infrastructure element from the users' perception of the quality of the underlying applications (unless the design of these is the responsibility of the cloud service provider too). In practice, it may be difficult to make this distinction.

It is obviously common for cloud service providers and their customers to be located in different jurisdictions. Where this is the case, two separate issues will need to be considered: the governing law of the contract and the applicable jurisdiction.

In relation to the governing law, the parties will usually expressly provide that the cloud computing contract is to be governed in accordance with the laws of a particular jurisdiction. Where the parties have not expressly chosen a legal system, the Rome Convention 1980 (*80/934/EEC*) (which will be replaced by the Rome I Regulation 593/2008/EC (Rome I) for contracts concluded after 17 December 2009) will apply. In the case of non-contractual obligations, such as tort, unfair competition or IP infringement, the Rome II Regulation 864/2007/EC (Rome II) will apply, while the Brussels Regulation 2002 and Lugano Convention 1988 will broadly apply to EU and EFTA (excluding Liechtenstein) jurisdictional issues.

The Rome Convention 1980 and the new Rome I provide that where there is no express choice of law, a contract will be governed in accordance with the law of the country in which the party who will perform obligations characteristic of the contract has its habitual residence or central administration. Furthermore, Rome I contains a specific rule providing that a contract for the provision of services shall be governed by the law of the country where the service provider has its habitual residence or central administration. In these circumstances, this will generally be the law of the place in which the cloud computing service provider locates its servers.

Rome II will apply to non-contractual obligations arising in "civil and commercial matters" between parties. Subject to a number of defined exceptions (including unfair competition, IP infringement, product liability and other circumstances where a specific deviation is defined), the law applicable to such obligations will be the law of the country in which the damage occurs or is likely to occur. This is a change from the law of the location in which the wrongful event took place, as had previously been applicable. As with contractual obligations, parties to a cloud computing contract may sidestep Rome II rules (concerning choice of law) by agreeing contractually on the law that will govern their non-contractual obligations. Care should be taken during cross-border dealings to ensure that foreign law does not give rise to unexpected, binding non-contractual obligations (for example, duties of good faith in negotiations which do not exist under English law).

If the document is used as a set of non-negotiable terms and conditions, the choice of governing law for non-contractual obligations may be ineffective. This is because this right of choice (provided by Article 14(1)(b) of Rome II) applies to agreements that are "freely negotiated". Although the meaning of "freely negotiated" has not been defined in Rome II, its requirement creates uncertainty over whether a non-contractual obligation governing law clause in standard form agreements will be effective.

Under the Brussels Regulation (which largely follows the form of the Brussels Convention 1968 and Lugano Convention 1988), a person domiciled in a contracting state may be sued in the courts of another contracting state where a contractual obligation is owed. A cloud service provider based in the EU can be sued in all the jurisdictions in which it provides services to its customers. The Brussels Regulation also provides for mutual recognition and enforcement of judgments. However, where the cloud service provider is based outside the EU, jurisdiction will depend on the relevant rules of court relating to service of proceedings on the service provider outside the jurisdiction.

Customers often take the view that the cloud computing contract should be governed by their local law as this is the legal system of which they have greatest knowledge. However, this will be difficult to negotiate (as service providers will not want a range of contracts across a global client base governed

by different legal systems), although if the customer is dealing as a consumer, the Rome Convention and Rome I Regulation provide that certain protection provisions of the law of the consumer's country of habitual residence cannot be contracted out of. Furthermore, it may not necessarily be the most advantageous position. If the cloud service provider does not have a sizeable presence in the customer's jurisdiction then any court order that might be obtained will be difficult to enforce in the service provider's jurisdiction. This applies particularly between EU customers and US service providers, and where there is a need to obtain emergency remedies against a cloud service provider: for example, if the customer considers that its data has been misused by the service provider. In these circumstances, obtaining emergency remedies will generally be more straightforward if the governing law of the contract is the local law of the cloud service provider.

Where the customer is a multi-national corporate, additional jurisdictional issues arise including:

IPR Licensing

Does the cloud service provider have the right to authorise the customer to use the software in all jurisdictions in which the customer operates? Quite often software licensing arrangements are country-specific and the service provider may not have obtained sufficiently broad sub-licensing rights to authorise the usage that the customer needs. As long as the customer notifies the cloud service provider of the extent of the proposed use, the IPR indemnity should give the customer protection in respect of a third party claim. However, this should be made part of the pre-contract due diligence enquiries and the customer should notify the service provider whenever it starts to use the cloud computing service from a new location. This is particularly important where the customer organises a central computer node for its overseas transmissions at its own premises, so that the cloud service provider only receives transmissions from the customer's central node and not from the overseas offices that were linked to the central computer node. In this situation the fact that the customer uses the service from a number of countries may not be apparent to the cloud service provider.

Local Law

The cloud services' customers need to be informed that use of the service in other countries is likely to be subject to the requirements of local law. For example, e-mails sent using the cloud computing service from an overseas country are likely to be subject to the local defamation law of that overseas country and data stored on servers is likely to be subject to local rules on data protection and disclosure for enforcement purposes.

Conflict of Laws

Both the cloud service provider and the customer need to be aware of problems caused by the inherently cross-border nature of the internet. As mentioned above, where a cloud computing contract does not specify the governing law or applicable jurisdiction (or where a court deems those specified to be inappropriate), such matters will be determined by private international law (or rules on conflict of laws). The application of private international law is potentially problematic, as its principles are dependant on the concept of "localisation" (that is, where in the physical world a particular element of a transaction occurred). Within the context of cloud computing contracts, adopting the "place of performance" for the purposes of localisation will, in many cases, produce odd and unpredictable results: for example, where the service is performed by software operating automatically; or where performance occurs on a server located in a jurisdiction different to that which the website (through which the cloud computing service's customers request the service) is stored. In theory, there is no limit on the circumstances in which a national government might claim to apply its laws and

regulations to the internet activities which originate in a different jurisdiction (although practical enforcement of those laws against a foreign enterprise is an entirely different matter). In practice, however, governments look to minimise the risk of a legislative "arms race" by applying the principle of "comity" (which essentially requires a state to refrain from applying its legislation to persons in another state unless it is reasonable to do so). However, as this principle is also rooted in the concept of localisation, its compatibility with cloud computing is highly questionable.

In light of this, the need for regulatory reform becomes all too clear. At present, the most promising alternative is the "country of origin" regulatory model (also known as "home country" regulation), whereby a cloud service provider would have to comply only with the laws of the country in which it was based. Whilst this model appears to "fit" the qualities of cloud computing better, in practice it may be extremely difficult to achieve. In addition, consumer lobbyists fear that the implementation of such a model would strip cloud services' customers of their statutory rights (as it would enable cloud service providers to migrate to countries with minimal consumer protection legislation). Similarly governments (especially those with strong cultural, political and/or religious agendas) fear a similar flight to countries with liberal content laws.

Data Protection

Data protection rules may apply at a local law level, particularly where personal data is transmitted outside the EU (see 'Compliance Issues' below for a more detailed review of the applicable data protection issues). The "safe harbour" rules relating to transmissions of personal data between the EU and the US have clarified the EU/US situation considerably. However, the situation in respect of countries other than the US is less clear.

Encryption Regulation

Encryption legislation stems primarily from the international level and derives from the potential for encryption devices or methods to be used for military, terrorist or criminal purposes, as readily as for commercial purposes; such devices or methods (categorised as "dual use" goods) will be subject to export controls by many countries. Of particular note are the US export authorisation and licensing requirements, which are far-reaching and require strict compliance. Where encryption mechanisms are used as part of the cloud computing service's applications, the export of encryption software from the US needs to be carefully monitored to ensure that the rules relating to such export are complied with, as the sanctions for non-compliance can be significant. Within the EU, export regulation of dual-use goods is a complex patchwork of EU legislation (namely Regulation (EC) 1334/2000) and national legislation, combined with international conventions. Despite the many similarities and overlaps, differences do exist between EU member states, particularly as regards administration and enforcement. As such, the competence of the EU is not exclusive and EU member states may require an export licence for dual-use goods even though they are not listed in EU legislation. It should be noted that as the rules (at state (in the case of the US), national and international level) change frequently, these need to be considered on a case-by-case basis.

Security Arrangements

One of the key concerns of cloud services' customers is the security arrangements that the cloud service provider will put in place. The following should be considered:

IT Security

The cloud computing contract should set out the IT security arrangements that the customer requires. The encryption of data prior to transmission between the customer's premises and the service provider's premises is particularly important, for example, where the internet is used for transmission. Customers may also require that their applications are hosted on hardware that is specific to them, rather than on "shared-use" hardware (shared between a number of the cloud service providers' customers). However, although this is an understandable security precaution, it limits the financial benefits of the cloud computing arrangement and restricts the use of hardware virtualisation methodologies.

Physical Security

The cloud service provider should be required to ensure that there is continuous physical security at its premises and that entry to the premises is limited to authorised personnel to reduce the risk of theft of equipment.

Personnel

The cloud service provider should be required to ensure that only personnel that have been security vetted have access to the service infrastructure. Suitable checks include records available through the Criminal Records Bureau. In particularly sensitive situations, the customer may want the right either to interview key support personnel, or to require that personnel it objects to are removed from the service provision arrangements but cloud service providers are likely to resist attempts to include such provisions.

Data Security

Cloud computing contracts should recognise that data loss and corruption will occur. The primary means of avoiding the worst effects of significant data losses is to ensure that back-ups are made at regular intervals by the cloud service provider and that these are tested at reasonably regular intervals to ensure that it is possible to reload the data.

If a loss of data occurs, the cloud based software set-up can then be reloaded from the latest available back-up. There will still be some data entered after the last back-up has been made that is irrecoverable but as long as the back-ups are made on a regular basis (usually daily) the loss will be relatively small.

As losses of data can have a serious impact on business, the provisions governing loss of data and limitation of liability will require careful negotiation and cloud services' customers need to ensure that data loss and corruption caused by the cloud service provider will amount to a breach of contract (these are habitually excluded in service providers' standard terms). However, where the cloud service provider is able to restore data from the back-ups it is arguable that as long as it does so within the time period stipulated in the cloud computing contract, the service provider should not suffer further liability to the customer. The customer may therefore have to accept that business

losses may arise both in relation to the period during which the data is being restored and in respect of any data that cannot be restored from the back-ups.

If the cloud service provider is unable to restore data from the back-ups then the limitation of liability will come under close scrutiny. Most limitation of liability provisions in cloud computing contracts will include both a financial cap on liability and an exclusion of indirect and consequential losses. From the customer's perspective the financial cap needs to be sufficiently high so that the costs of re-inputting data manually will be recoverable. The exclusion of indirect and consequential losses should also be clarified so that the costs of data re-inputting are not excluded from recovery. The issue of whether or not the customer will have any basis for claiming the business losses from the cloud service provider in the event that data is not recoverable is largely a matter for negotiation. However, where contracts are entered into on written standard terms the requirement of reasonableness under UCTA is applicable.

Data Protection & Security

The Eighth Data Protection Principle

Where the cloud computing service is hosted in the UK or within the EEA (which comprises all EU countries plus Norway, Iceland and Liechtenstein), the customer will need to comply with the eight data protection principles contained in the Data Protection Act 1998 (DPA) if any personal data it holds could be input or transferred to the cloud service provider's servers. It is the responsibility of the customer, as data controller, to ensure compliance with the DPA and relevant guidance from the Information Commissioner's Office (ICO). This includes ensuring that the seventh data protection principle under the DPA is followed when it appoints a data processor – i.e. that a good supplier is chosen, their services are audited and the contract enforced with regard to security measures.

Additional data protection requirements may apply in order to comply with the eighth data protection principle if any data is "transferred" outside the EEA. This may occur if, for example:

- The cloud computing service is hosted outside the EEA; or
- A support or maintenance provider with access to personal data is located outside the EEA; or
- A customer user accesses personal data on the cloud computing service remotely from outside the EEA or takes personal data from the cloud computing service on a laptop outside the EEA.

Although the DPA does not define "transfer", ICO guidance states that, for data protection purposes, it should assume its ordinary meaning: that is, the transmission from one place, person etc to another. "Transfer" does not mean the same as mere transit. Therefore, the fact that an electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country, does not bring this transfer within the scope of the eighth data protection principle.

In order to comply with the eighth data protection principle, the data controller must establish whether the importing country ensures an adequate level of protection for the personal data, considering the circumstances of the transfer. The data protection regimes of some non-EEA countries (Guernsey, Jersey, Isle of Man, certain organisations within Canada, US safe harbour organisations, Argentina and Switzerland) have been approved by the European Commission as providing adequate protection so transfers to such countries are acceptable, but if transfers are being made to any other countries, the data controller must find another way of satisfying the eighth data protection principle.

This can be difficult with cloud computing services as service providers may use a number of server farms in different locations and do not always provide information on where data will be held but it is common for cloud computing service providers to host servers within the EEA or be registered as US safe harbour organisations.

Data controllers are free to make their own assessment of whether a country offers an adequate level of protection and the Information Commissioner has provided some guidance as to the types of factors which would need to be taken into consideration. If "sensitive data" will be transferred and this will be processed on a long-term basis, a higher standard of protection and an in-depth assessment of the circumstances of the transfer will be required, including evaluation of the legal system in force in the country of importation.

If the importing country does not offer an adequate level of protection, other safeguards can be put in place to allow the data transfer. These can include the use of binding corporate rules or the use of model contracts authorised by the Commission.

Binding corporate rules are intended to operate as a form of internal data protection law within an organisation. However, they are designed to work for transfers within a group of companies rather than between a data controller and its external suppliers. They are also cumbersome and difficult to implement so are unlikely to be a realistic solution for cloud computing.

The model contracts impose obligations on both the exporter and importer of the data and enable data subjects to enforce their rights as if the data were held in the EEA. Under the model contract for data transfer from a controller to a processor, the data exporter is liable to the data subject for any breach by either party except in limited circumstances. However, the data importer is required to indemnify the data exporter to the extent of its liability to the data subject.

In addition to satisfying the eighth data protection principle, it is important that individuals are notified that their data may be transferred outside the EEA in order to ensure that such processing is fair and lawful.

The Seventh Data Protection Principle

Most IT services agreements assume that the supplier will act as data processor for the customer and include a clause stating that the supplier will put in place appropriate technical and organisational measures to keep any personal data secure. This is to satisfy the requirements of the Seventh Data Protection Principle, which requires the data controller to ensure that the data processor is appointed under a written contract, and also that the data processor has adequate information security procedures in place. The customer may wish to impose further requirements on the supplier particularly in relation to the security of data. This may include imposing controls on how the supplier holds the data and audit rights to check that these controls are in place.

In such agreements, the supplier is a data processor rather than a data controller as the supplier will process the data in the manner directed by the customer. However, in some circumstances in cloud environments, cloud services providers may wish to take certain actions in respect of the data without necessarily consulting with the customer on each occasion. For example, a cloud service provider may wish, for disaster recovery or load balancing purposes, to move the data between servers at different sites or to servers which are owned by different group companies or which are located in different countries. In these situations, it will be necessary to consider whether the cloud services provider's actions would make it a data controller rather than a data processor.

According to the definition in the Data Protection Act, a data controller must decide **the purposes** for which the personal data are or will be processed and **the way** in which the personal data are or will be processed. In the Information Commissioner's view, it is the determination of the purposes which is paramount. There is therefore some scope for a company to have some discretion in determining the way in which the data are processed, but not the purposes of the processing and to remain a data processor. Cloud services providers may therefore be able to rely on this view for some activities which they plan for data management. However, this is a grey area and if a cloud services provider is, in reality, also involved in determining the purposes of the processing (either alone or jointly with the customer), then it is likely to be considered to be a data controller and will be responsible for compliance with Data Protection Act.

If the parties are acting together in determining the purposes for which and the way in which data will be processed, they will be joint data controllers and will be jointly liable for any breaches of the Data Protection Act.

As a data controller, a cloud services provider will need to consider notifying the Information Commissioner about its processing activity and both parties would need to consider what data protection notice (under the Fair Processing Code from the First Data Protection Principle) notices have been given to users with regard to the fact that the cloud services provider is a joint data controller with the customer.

If there is a possibility of the customer and supplier being joint data controllers, detailed data protection advice should be sought so that the correct position and relationship can be ascertained and the data protection clauses can be amended accordingly to address the risks which arise.

Markets in Financial Instruments Directive 2007 (MiFID) and Sarbanes-Oxley Act 2002 (SOX)

Where a cloud services customer is subject to MiFID and/or SOX regulation, they will need to be mindful of how their use of cloud computing may impact their ability to comply with MiFID and/or SOX requirements.

MiFID is an EU directive that aims to increase consumer protection in the investment industry by increasing competition and transparency. Similarly, SOX (a US Federal Law) also aims to increase transparency within the investment industry; however, its focus is on reforming internal control processes and the manner in which these are audited.

With regard to MiFID compliance, the cloud services customer will need to consider whether it has the capacity to: conduct a proper due diligence on the cloud service provider's finances and expertise; ensure that the cloud service provider supervises its performance, manages associated risks and discloses any developments which may compromise the service(s) provided; retain all records for a period of 5 years; and retain a right of access for itself (as well as its auditors, the Financial Services Authority and any other appropriate regulator) to data related to the services and to the cloud service provider's premises.

Similarly, with regard to SOX compliance, the cloud service customer will need to consider whether it has the capacity to: ensure that the cloud service provider incorporates a comprehensive set of controls that are internally assessed by the service provider's staff and external auditors on an ongoing basis (to ensure operational effectiveness); maintain visibility of data; ensure efficient document management; document all internal control processes; and allow both internal and external auditors to test such processes.

The parties should check that all the following issues are covered in the Cloud Computing agreement, as appropriate:

- Basic monthly service charge
- Separate licence fee(s)
- Price per seat/user
- Service levels, service credits and termination thresholds
- Configuration assistance
- Price for configuration assistance
- Basic support/maintenance charge
- Features of basic support/maintenance
- Price for premium support/maintenance
- Features of premium support/maintenance
- Seat/user limit
- Price for extra seats/users storage limit
- Price for extra storage back-up and business continuity
- Escrow of object code
- Price of object code escrow
- Escrow of source code
- Price of source code escrow
- Escrow of data
- Price of data escrow
- Features of transition services at termination/expiry
- Price of transition services at termination/expiry
- Other chargeable elements
- Price of other chargeable elements



Roger Bickerstaff

Partner

Roger is Joint Head of Bird & Bird's International IT Sector Group. Roger advises on all aspects of IT law to public and private sector clients, but he has a particular interest and experience in advising on public sector IT projects. Roger also has a significant level of expertise in public procurement law.

Roger has over 15 years experience of advising on large-scale IT projects in both the public and private sector. This wealth of experience means that he understands the issues that arise in major projects and can provide the solutions to resolve these issues. He now fulfils the role of trusted advisor on a range of significant projects, providing advice that goes well beyond legal and contractual matters, and into the technical and commercial heart of the success of the implementation of projects.

Roger is recognised as being a leading exponent of IT law and is regularly cited within the legal directories, particularly for his public sector practice. The 2008 Chambers & Partners directory commented, "Roger Bickerstaff commands a 'great reputation on public sector IT work'."

Tel: +44 (0)20 7415 6000
Fax: +44 (0)20 7415 6111
Direct: +44 (0)20 7415 6160
roger.bickerstaff@twobirds.com



Barry Jennings

Associate

Barry Jennings trained at Bird & Bird and qualified into the commercial department in September 2004. He advises public and private sector clients on a full range of commercial legal issues, including outsourcing and off-shoring, contract management, drafting and negotiation of contractual documents, intellectual property, software and data licensing, procurement regulations, data protection and compliance with consumer protection legislation.

Barry chairs the firm's Technology Knowledge Group, helping keep Bird & Bird lawyers briefed on key technology trends and topics, and is a member of the Society of Computers & Law, Intellect and ITS(UK). He also co-edits the e-commerce chapters of Sweet & Maxwell's Encyclopedia of IT Law and is a member of NAO's PFI Contract Managers' Forum.

Barry has written articles on IT Virtualisation, PFI/PPP agreements, intelligent transport systems and telematics, plus speaks regularly on the legal and commercial aspects affecting a range of technology topics (including IT & Software Virtualisation, web 2.0, cloud computing, net neutrality, rapid application development and IPTV).

Tel: +44 (0)20 7415 6000
Fax: +44 (0)20 7415 6111
Direct: +44 (0)20 7905 6382
barry.jennings@twobirds.com