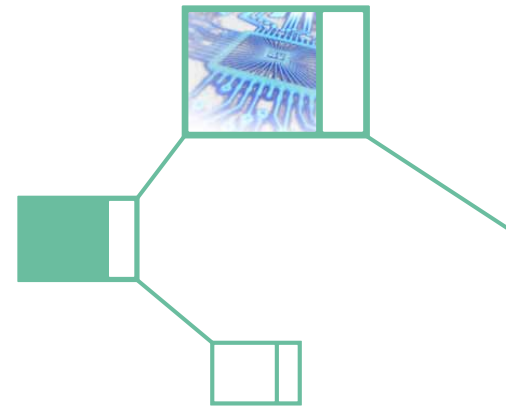


Cloud computing



Although cloud computing has become one of the hottest topics within the IT world over the past few years, a consensus on how it should be defined still eludes the industry. A key reason for this is because so many interested parties use the term to encompass different IT functions. Despite this, many businesses - service providers and customers alike - are investing in or at least investigating cloud computing, even at this early stage in its development. For those businesses interested in cloud computing, this note attempts to provide a high level definition of it, outlines some of its benefits, and then presents the most significant risks and legal issues that should be considered.

What is cloud computing?

Most experts agree that cloud computing is not a new technology, but a new way of supplying IT resources via the internet. As a computing model, it can be seen as an evolutionary step on from the Application Service Provider (ASP) model, having come about through the confluence of a number of trends in the market. These include the increasing reliance of businesses on IT systems; the associated movement towards outsourcing IT functions to harness greater computing power while reducing costs; advances in storage and networking technology; the move to distributed data storage models for potential business continuity benefits; and the increased availability of high speed broadband for businesses.

Analysts at Gartner define cloud computing as a style of computing in which massively scalable IT-related capabilities are provided 'as a service' using internet technologies to multiple external customers. The 'cloud' can refer to public, community or private networks, or a hybrid of two or more types of cloud. The term cloud computing is often used to refer to different service models; e.g. infrastructure as a service (IaaS), where the supplier provides virtualised networks, storage and systems software; platform as a service (PaaS), i.e. virtualised servers; software as a service (SaaS), where software applications are run through a web browser; and database as a service (DaaS).

Benefits of cloud computing

Common characteristics of cloud computing services are often highlighted as important benefits in themselves. For example, their agility, flexibility and scalability can allow businesses to access them readily and increase or decrease requirements on demand, improving efficiency of resource utilisation (with associated environmental benefits).

The potential cost savings from using cloud computing services can be compelling, especially for SMEs. Resource pooling allows smaller businesses to benefit from economies of scale by enabling access to enterprise-level IT resources at a fraction of the cost that would otherwise be incurred in acquiring such resource. Additionally, services are often paid for on a subscription basis, reducing and sometimes eliminating the need for upfront capital expenditure, long-term software licensing costs and ongoing maintenance and upgrade costs that can be involved in traditional IT solutions. Importantly, this can reduce business start up costs.

Risks and legal issues

Along with the benefits, however, there are a number of risks and legal issues associated with cloud computing. While these will vary depending on the type of cloud service and the deployment model, those discussed below will need to be considered for most, if not all, cloud computing models. Surveys show that many businesses are already aware of at least some of these risks, which include security breaches and service outages, and are wary about utilising cloud computing because of them. This is understandable: when things go wrong in the cloud, there may be major adverse effects for the customers of the cloud service including the potential for litigation and damage to reputation. Yet these risks need not be insurmountable hurdles for some businesses, nor outweigh the potential benefits of using cloud computing.

Key to a successful cloud computing project is the careful consideration of the relevant risks in the early stages of planning - rather than as an afterthought - and the development of sound risk management strategies. As the cloud computing standards in the industry are currently

Our team



Graham Hann
London
+44 (0)20 7300 4839
g.hann@taylorwessing.com



Louise Taylor
London
+44 (0)20 7300 4220
l.taylor@taylorwessing.com



Sally Annereau
London
+44 (0)20 7300 4994
s.annereau@taylorwessing.com

immature, businesses should also undertake due diligence of cloud computing providers to evaluate the practical and legal risks of moving to a particular cloud or clouds. Input from lawyers from the outset can help businesses with their selection process, as well as help them to identify legal risks and address them – where possible – in negotiations with the provider and implement appropriate risk mitigation strategies.

Security

Security is often cited by businesses as a chief impediment to moving to cloud computing. Data in the cloud can be exposed to risks of unauthorised disclosure as a result of security breaches, particularly where the data is unencrypted. Breaches could have major negative repercussions on a cloud customer's business, especially where data in the cloud contains confidential information, intellectual property or personal data, or where the cloud computing service is business critical or customer facing. Such consequences include negative publicity and costly third party claims such as breach of contract or breach of confidence.

These security concerns have led to the Common Assurance Metric (CAM) initiative, backed by the European Network and Information Security Agency and cloud providers such as eBay and Microsoft. Its aim is to create a set of standards that measure the security of cloud computing services objectively, and it is expected to have the outline of the CAM ready by the end of 2010. Until any such standards are in place though, cloud customers will need to seek assurance from providers that they have implemented and maintain adequate security practices to mitigate risks to customers. Meanwhile, market forces may help: given that customers can choose between a number of different cloud providers, there may be some incentive for providers to guarantee, as a market differentiator, the integrity and resilience of their cloud solutions.

In any case, cloud computing customers will need to ensure that security is a top priority from the start and due diligence is conducted before selecting and contracting with a cloud provider. Questions to consider during this process include:

- how data is stored by the cloud provider (e.g. whether it is co-mingled with other customer data);
- whether the provider can offer assurances that any personal data will only be processed in accordance with the customer's instructions (e.g. that it will be deleted on request);
- whether encryption is used / permitted;
- whether the provider has any relevant industry accreditations, such as ISO27001-2005;
- what the provider's current security measures are and whether it maintains a security plan;

- how the provider monitors and reports security breaches;
- how the provider responds to breaches and aims to prevent future breaches; and
- whether the customer has access to any security audit reports or other evidence of the provider's security track record.

If a cloud provider does not offer a customer the security assurances it seeks, the customer will need to (a) accept some risk and implement appropriate risk mitigation strategies; (b) look for another provider; or (c) consider whether the particular cloud computing service is appropriate for its intended use. Ultimately, for some types of data and in certain sectors (such as the financial or health sectors), customers may decide that – at the moment - the risks of cloud computing outweigh its potential benefits.

Data protection

Using cloud computing to process personal data or moving personal data to a cloud may expose a cloud customer to the risk of non-compliance under data protection legislation.

A cloud customer will usually be the data controller of personal data, and will therefore be responsible for compliance with data protection legislation. In the UK, the Data Protection Act 1998 ("DPA") will apply where the data controller is established in the UK or where the data controller is established outside the EEA but the equipment used to process personal data is located in the UK. The two main DPA compliance issues in these circumstances are as follows:

(1) Security obligations

A cloud customer, as data controller, has an obligation under the DPA to ensure that the cloud provider, as data processor, has adequate technical and organisational security measures in place and gives sufficient contractual warranties in respect of those security measures. If the cloud provider's security measures are inadequate or the contractual protection offered is insufficient, the customer would either need to negotiate with the provider or find a provider that does offer adequate assurances. If the cloud provider cannot assist the cloud customer to meet its obligations as data controller under the DPA, the cloud customer (and not the cloud provider) could potentially face fines of up to £500,000.

(2) Transfer of data

When personal data is moved to the cloud, it may be stored in multiple jurisdictions around the world. This key characteristic of cloud computing brings a number of its benefits; e.g. it can minimise the effect of a serious IT failure on a single site. Yet it also raises a DPA compliance issue. Under the DPA, data controllers cannot transfer personal data outside the EEA unless either the destination country offers an

“adequate” level of protection for individuals’ personal data or one or more pre-conditions are met such as: (a) they have obtained informed consent from the data subjects for that transfer; (b) where the cloud provider is in the US, it is certified under the FTC-enforced Safe Harbour regime; or (c) adequate contractual protections based on European Commission approved terms are in place with the cloud provider.

Businesses will need to involve lawyers to determine which legitimising option is the most feasible in the circumstances. This will depend on a number of factors, including the number of data subjects (as a large number of data subjects may make it impractical to obtain informed consent); which country or countries the data will be processed in; where the cloud provider is located; whether the cloud provider’s standard terms adequately cover DPA obligations and, if not, whether the customer can negotiate DPA-compliant terms.

If the selection of a certain cloud provider will mean that the customer is not able to comply with the DPA, there are other options. For example, the customer could choose another provider or anonymise personal data before moving it to the cloud (when doing so will not reduce its value to the business; e.g. in the case of certain marketing information). The business could also decide to keep all personal data out of the cloud; at least until compliance issues have been resolved.

DPA: good practice guidelines

The Information Commissioner released a draft Personal Information Online Code of Practice in December 2009 as a consultation document, which covers the use of cloud computing facilities to process personal data. The draft Code also provides good practice guidance to help organisations comply with the legal requirements of the DPA; e.g. by ensuring that an organisation’s privacy policy reflects who it is sharing its data with, assessing risks of security breaches occurring and the potential harm to individuals, and putting in place a plan to deal with security breaches. SMEs, in particular, may find this document a helpful starting point when considering their obligations under the DPA. The consultation closed on 3 March 2010 and the finalised Code of Practice is expected to be available by Summer 2010.

Loss of data / portability

The European Network and Information Security Agency released a report in 2009, which identified lock-in as a significant cloud-specific risk. It said that there is currently “little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability.” This lack of standards for data

portability introduces dependency on a particular cloud provider by making it potentially difficult for the customer to migrate from one provider to another or migrate back in-house. It also makes it difficult to remove data quickly if required; e.g. for an external audit or if the cloud provider becomes insolvent or stops providing cloud computing services.

Concern over this issue has prompted discussions about a potential ‘open cloud’ where providers can interoperate readily and customers can move or retrieve their data, or switch from one service to the other, with ease. In the absence of such standardised cloud services at the moment, however, during the process of selecting a cloud provider businesses will need to consider questions such as:

- how the data is stored, and how quickly data can be retrieved by customers from the cloud;
- whether the provider can do a complete data restoration if necessary, and how long this would take; and
- whether data can be retrieved in a format that is compatible with different providers’ systems.

Contracts

Currently, providers tend to present their standard terms and conditions on a ‘take it or leave it’ basis, and may not provide sufficient assurance to customers on key issues such as security, data transfer or access to the customer’s data. Cloud providers are also likely to limit their liability in the event of outages, poor performance, loss or corruption of data or breach of confidentiality. Also, if a customer selects a specific provider following due diligence, it may want the right to terminate on change of control of the provider and restrict the provider’s ability to assign the contract to third parties, but it is unlikely that a cloud provider will offer these provisions in its standard terms.

Larger companies may have sufficient bargaining power to negotiate key concerns with a provider, but SMEs may not be able to do so. This means that, rather than negotiating a position they are comfortable with, SMEs are likely to have to evaluate different providers and their standard terms and conditions and either select the cloud provider that best meets their requirements or - depending on the importance of the service to its business - consider other IT solutions outside the cloud.

Service availability

Businesses are often concerned about the reliability of cloud computing given its dependence on the internet for connectivity and the potential for outages and loss of data. This issue is particularly relevant for SaaS key applications (such as customer facing applications and process management software) and data storage via IaaS.

Businesses will need to evaluate any service level agreement (SLA) offered by cloud providers, as meaningful service levels and service credits can go some way to mitigating the risks inherent in the cloud by providing an incentive for the service provider to perform. However, some providers may not offer any SLA and others may propose SLAs which are inadequate for a customer's specific needs. Cloud providers will also usually try to exclude their liability for loss or corruption of data, whether or not it is suffered as a direct result of service failure.

Again, whether a customer can negotiate the cloud provider's standard terms to tailor them for the customer's specific service level requirements will depend on the relative size and bargaining power of the parties. In any event, however, it is important to remember that SLAs do not address the practical risks of loss of uptime, and customers will need to implement their own internal risk mitigation strategies to minimise the impact of downtime or outages on their business.

The first way of mitigating risk is to assess the cloud provider's service availability track record, business continuity and disaster recovery plans and its contractual commitment to improving services and dealing with availability problems. Second, the customer should implement and maintain its own business continuity and disaster recovery plan, and address the cloud provider's role in this plan. A customer should also ensure that it has the right to terminate the contract in the event of service level failures to enable it to transfer to another provider (or in-house) without financial penalty if it is not satisfied with the provider's performance.

If the customer still has significant concerns about uptime and outages, it may decide to delay its use of cloud computing for business critical applications or services, at least until it has had a chance to evaluate the cloud provider's performance in respect of non-critical services.

Putting data / IP in cloud

Before sending any licensed data or intellectual property into the cloud, businesses should check that they have the right to do so, as there may be restrictions in the original third party licence (e.g. territorial limits on licence, disclosure to third parties).

Industry specific regulation

Industry-specific regulations may impose additional obligations on organisations such as those operating in the public, financial or health sectors. These may have an impact on any decision to move to the cloud, and may determine whether the proposed move to a particular cloud provider – or the cloud itself – is appropriate.

Insurance

Customers may need to check with their insurers before moving to the cloud to ensure that they will remain covered for loss of data, third party claims and other risks arising as a result of the customer's use of the cloud service.

Certification

If a cloud customer is in the process of achieving industry certification, this may be jeopardised by a move to the cloud if, for example, the cloud provider does not meet certain standards (or cannot provide evidence of compliance with the required standards) and / or if the customer is not contractually entitled to audit the cloud provider. This needs to be considered in the early stages when selecting a cloud provider and addressed by the customer in its internal risk mitigation strategies.

Conclusion

On top of evolving cloud computing standards and the absence of a clear industry standard definition of cloud computing, businesses moving to the cloud are faced with significant business risks. Nevertheless, the potential benefits of cloud computing, especially for SMEs looking for major cost savings, may outweigh these risks. The key to determining whether the move is worthwhile - and if so, which cloud provider / deployment model is the most appropriate - is a careful consideration of the risks and benefits.

www.taylorwessing.com

Berlin Brussels Cambridge Dubai Düsseldorf Frankfurt Hamburg London Munich Paris Beijing^Q Shanghai^Q Warsaw^A

© Taylor Wessing 2010

^QRepresentative offices

^AAssociated office

This publication is intended for general public guidance and to highlight issues. It is not intended to apply to specific circumstances or to constitute legal advice. Taylor Wessing's international offices operate as one firm but are established as distinct legal entities. For further information about our offices and the regulatory regimes that apply to them, please refer to: www.taylorwessing.com/regulatory.html

NB_000066_12.10