

Is your head in the clouds?



What is cloud computing?

Cloud computing can mean different things to different people. In simple terms, the computer hardware and software which currently resides on your business' network or on your desktop is actually provided as a service, typically by a third party and accessed directly over the internet. Exactly where the hardware and software resides and how it all works is largely hidden from the end user, it's somewhere up in the nebulous "cloud" that the internet represents!!

What have we learned about the cloud?

The cloud is not immune, so outages, data loss and security breaches will occur. Some of the largest cloud players including Amazon, Google, Sony and Microsoft, have all suffered significant downtime and associated costs; affecting the availability of systems and data, which in-turn has had a negative impact on numerous businesses and thousands, if not millions of users. Cloud computing is however an increasingly common approach for providing an IT service, so what should you consider?

“Sony PlayStation Cloud Computing Network Hacked and Personal Data Stolen”
 The external intrusion resulted in personal data loss and the cloud network being offline and unavailable to over 70 million users for 25 days.

“Amazon’s Cloud Computing Crash Wipes Customer Data”
 Thousands of businesses, major websites, valuable customer data lost and millions of users impacted by outage.

“Microsoft’s Sidekick cloud outage”
 T-Mobile Sidekick outage lasted for a week-long, leaving users with no access to email, calendar and the other personal data. To add to the fiasco, Microsoft confessed that it lost cloud-stored data bits and were not be able to restore them; and they had no backups!

“Software Bug Brings Down Google’s Cloud Email Service Gmail”
 Gmail users awoke to find messages in their Google Gmail inbox, folders and other data vanished. At its peak, the outage affected roughly 150,000 Gmail users. Consequently, the affected accounts were restored from tape back-up.

The Brighter Side of Cloud Computing:

Companies are considering moving to the cloud computing model for a number of reasons, including:

- 1. Flexibility** – The different levels of exposure in the cloud (Software As A Service (SAAS), Infrastructure As A Service (IAAS), Platform As A Service (PAAS)) offer companies the ability to expand and contract as demand grows making it easier to manage capacity and costs.
- 2. IT Strategic alignment** – Moving to a cloud computing model allows IT functions to focus their resources from fire-fighting and tactical fixes to innovation and business enablement.
- 3. Cost saving** – It enables you to move from a capital investment to an incremental operational expense, and requires fewer in-house IT resources to provide system support. Not to mention the additional cost savings as a result of the change in disaster recovery model.
- 4. Improved disaster recovery and backup** – Technology management is the responsibility of the technology provider. They have to provide appropriate controls to protect the data, fault tolerance and disaster recovery.
- 5. Mobile accessibility** – Current research indicates that over a third of adults in the UK are using smartphones, and this trend is likely to increase in the coming months. The cloud enables the mobile workforce to access data from virtually anywhere.

The Darker Side of Cloud Computing:

Companies are now re-evaluating their cloud strategies, some reasons for this include:

- 1. Service availability** – Just as the conventional outsource model has come to grips with defining and firming up Service Level Agreements (SLAs); cloud computing has introduced an entirely new level of complexity, as more and more companies are starting to discover that SLAs currently being quoted by cloud providers are not being met. There may also be many intermediary providers that a company relies on to access their cloud hosted applications and this makes any guarantees of service uptime less concrete.
- 2. IT migrations and project complexity** – Typically a company's IT infrastructure has been built up over years of changes, acquisitions and bolt-ons creating a complex web of interconnected applications and

technology assets; this results in increased complications when moving these to cloud platforms as these will have to fit with the cloud providers application architecture, thus also increasing the project costs. As yet we still haven't seen the next wave of any outsource model moving from one cloud provider to another!

- 3. Application performance** – Cloud computing relies on the performance of internet connections. With the majority of business applications not being designed to be used in a cloud model, there will be an inevitable impact on performance.
- 4. Data Security** – The success of information security awareness programs over the years has resulted in CIOs becoming more risk aware and increasingly uncomfortable with handing over their critical data to an external provider.
- 5. Data Privacy Regulations** – Laws and regulations regarding Data Privacy can vary significantly from jurisdiction to jurisdiction - what may not apply in one country may still be relevant in another - therefore it is important to ensure that you know exactly where all instances of your data resides.



Challenges with Cloud Computing

- 1. Data Governance** – Business data needs to be accessed, monitored and protected. Data and the information subsequently generated, is the “life blood” of most businesses. So the question that should be asked is, “How much loss of control over your data are you willing to accept?” On top of all of this, businesses are required to comply with numerous legal and regulatory requirements. By moving the data into the cloud, the business may not

be able to achieve the same level of control they previously afforded over their data. They would instead have to largely rely on the service provider to guarantee the security of their data.

- 2. Data Protection** – A business located in the UK will be subject to the Data Protection Act 1998 when handling personal data. If a business decides to use cloud computing it needs to ensure that its cloud computing services comply with the Act. Cloud computing relationships can be complex and involve the transfer of data across multiple jurisdictions.

As the Data Controller, the business is solely responsible for compliance with the Act and ensuring appropriate contractual requirements are in place with third parties. This includes the obligation to ensure that they retain close control over their personal data, even when the data is being processed on their behalf; furthermore, businesses need to be aware of the local laws which may apply to the data which resides within the cloud. This raises, for example, concerns about access to data in the US under the Patriot Act.. However, the more obvious data protection issue relates to the distributed nature of the data within the cloud computing service. Do you know where your data is all the time?

- 3. Compliance** – The US Sarbanes-Oxley Act (SOX) and the EU Data Protection directives are just two of many compliance requirements which can affect data handling in a cloud computing environment. The EU has legislative backing for data protection across member states, but in the US it can be far more complex as it varies from state to state. Furthermore, if your business deals with payment card transactions then you are going to be subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS) which requires additional consideration when selecting your cloud provider.
- 4. Data Migration** – Another challenge with cloud computing is data migration. When a user or business wants to change their cloud provider, you should be aware that there is no defined standard between the providers and as such, change can be complex. There can be difficulty ensuring that data is appropriately and completely deleted where required. For example, in the event of a cloud provider becoming bankrupt or ceasing its services, this is likely to be problematic when determining exactly what and whose data is residing where and how this can be retrieved. Understand the financial stability of your cloud provider.

- 5. Service Availability** – Given the recent outages suffered by Gmail, EC2 etc. it's imperative that organisations have provisions in place with their cloud host to provide the level of service availability required by the business. SLAs typically don't provide the required enforceable guarantees - SLAs will typically not cover a business loss. As such it's critical that you have clearly defined and enforceable contractual clauses with the cloud service provider which cover this in the event of a prolonged loss or reduction in service availability. Make SLAs contractually binding and check the cloud provider's Business Continuity arrangements.



Overcoming Cloud Computing Challenges

When considering moving to a cloud based environment, the challenge for the business is to try and retain the integrity over the controls, transparency and rules that existed prior to the cloud solution. Therein lies the problem!! Time and again, companies are preparing to move to the cloud before they have actually achieved effective data governance in their existing environment. Below are five key steps to consider when you're looking to set-up and execute your migration to the cloud:

- 1. Define and Document Rules** – Put in place a complete inventory of the rules by which data is to be governed. The rules must be functional and include mechanisms for performance measurement and data reporting. Only when these rules are written can one evaluate the impact of a cloud-based solution.
- 2. Test reporting** – The reporting functions must be tested to ensure they provide accurate information in respect of how data is used, or misused, within the business.
- 3. Demonstrate transparency** – Management is entitled to know what the reports contain. By using the reports

to communicate with management, you are creating transparency and also building the appetite for those reports to continue, whether or not a cloud solution is deployed.

4. **Educate the lawyers** – Lawyers drafting and negotiating cloud service contracts need to understand what the organisation requires to ensure that it complies with its legal and regulatory obligations and continues to align with its governance framework.
5. **Manage the Request for Proposal (RFP)** – The RFP should clearly define the control requirements expected from the cloud provider. It should stipulate the provider's responsibilities with respect to enforcing the rules, capturing data and reporting the results.

How Kingston Smith Consulting Can Help

Our team bring expertise and experience to every engagement. Every consultant in our team has a record of successful delivery in their field of expertise. By employing the experienced staffing model we are able to deliver solutions that focus on achieving a return on investment based on your specific needs.

- **Due Diligence** – Because cloud computing involves outsourcing an application, data, infrastructure or function to a third party, cloud computing relationships inherently involve risk. To mitigate the

inherent risks, our due diligence review encompasses the financial, environmental, business and technical capability and validity of the vendor, enabling our clients to make informed decisions.

- **Compliance** – Given data in a cloud environment has to physically exist on servers somewhere in the world, the locations of these servers are subject to different privacy and data management laws in various countries. Our team are highly experienced practitioners in the field of global data protection and information security and can perform pre- and post-compliance assessments with respect to the relevant data protection laws and regulations.
- **Audit** – Moving to a cloud solution also involves relinquishing or transferring a certain level of control to the cloud provider. Thus, it's paramount to ensure they can provide your organisation and/or regulators with continued reasonable assurance over your controls. We can assist you by performing an audit of your vendor's controls whether outsourced or co-sourced. Audits include evaluation against risk, control and legal and regulatory requirements such as Sarbanes Oxley, Data Protection Act, Basel II, MiFID, HIPAA, PCI DSS, CRC etc.
- **Supplier Selection / Contract Review** – The provider selection process can be a daunting undertaking. We can help you analyse your business requirements, search for prospective providers, facilitate the selection process and support you with your contract negotiations.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice of the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD