DAV management

redefining the management of change

Look before you leap

Why due diligence and commercial management are a prerequisite for safe and effective Cloud solutions

DAV Management Limited

http://www.davmanagement.com

Copyright

Look before you leap

Over the past 4 years we have seen the irresistible rise of Cloud Computing. This term is given to a business model for computing, where capacity for business solutions, data storage and networking can be dynamically acquired, on demand, and paid for according to usage. The major benefits of this model are that new services can be introduced, relatively quickly, without recourse to lengthy capital procurement processes, or challenges in locating physical space or power in a Data Centre. In fact, all that's needed is a credit card to get the ball rolling! And that's where the problems start. In this article, we explain why organisations considering a Cloud strategy must take due diligence seriously and why commercial management will be a fundamental element of any successful delivery.

1. A computing paradigm for the future

Cloud Computing has been described as arguably the third revolution of IT, following the Personal Computer and Internet revolutions. Global Software as a Service (SaaS) revenues are forecasted to reach $106bn in 2016, increasing 21% over projected 2015 levels. A Goldman Sachs study published earlier this year projected that spending on cloud computing infrastructure and platforms will grow at a 30% CAGR from 2013 through 2018, compared with 5% growth for the overall enterprise IT.

The Cloud revolution seems unstoppable. Yet despite increasing levels of acceptance there is still a degree of apprehension in some markets, perhaps even a lack of confidence and some false starts.

Cloud based services are all around us and are increasingly pervasive in consumer life, with the explosion of services like iCloud from Apple and Microsoft's OneDrive. For those not familiar with the platform, Cloud Computing denotes the outsourcing of IT functions over the internet so that both hardware and software services can be provided remotely on an as-needed basis, rather than through a physical IT infrastructure. Consequently, an advantage of Cloud Computing is that a user`s location and IT infrastructure is largely irrelevant.

Many CIOs are in the process of moving applications and services into the Cloud. Some are considering Cloud-based computing due to economic reasons, while others are looking to create new IT services. Regardless of the reasons, one of the challenges that CIOs still have to face is how to ensure they are able to put in place appropriate and effective contract terms and an associated service level agreement, that protects vital elements of their business, such as data security, IP infringement, and motivates the provider to deliver the optimum level of service for the best possible price. It's a similar challenge to that presented by outsourcing just a few years ago.

In fact, there are probably only two real differences between Cloud Computing and traditional IT infrastructure outsourcing: shorter contracts – in some instances hours, days or weeks rather than months or years; and no upfront costs, with CAPEX and installation absorbed into rental charges.

The main benefits for business in adopting a Cloud based approach are:

- Cost savings - the Cloud Computing model offers organisations the prospect of outsourcing the procurement and maintenance of IT services which will allow payment for services on a "pay as you go" or subscription basis, based on the amount of service actually used; at the same time, this offers the potential of significant savings in capital investment as increasingly major capital expenditure on IT infrastructure will be borne by the Cloud Computing suppliers, rather than by users. Finally, there will be opportunities for reducing IT teams and transferring IT personnel to those suppliers.
- Flexibility - the Cloud Computing model allows key suppliers to have sufficient bandwidth in place enabling them to combine demand from different businesses across different sectors in different time zones, to significantly reduce the total amount of computing capacity needed. This, in turn allows users to meet peak demands, quickly and more cost effectively as they no longer need to install costly IT infrastructure that is frequently not used at full capacity for much of the time.

2. Before you take the plunge

The reality is that Cloud Computing is still relatively new, it's fashionable – suppliers offering Cloud based services have well developed propositions and are keen to see a return on the investment made in getting there. It's moving quickly towards the mainstream. And for organisations considering utilising it, that places a hefty premium on something we've seen before: commercial management, supplier evaluation and due diligence.

Indeed, the issues for organisations, however, are exactly the same issues faced when outsourcing, but multiplied many times over because Cloud (especially using external cloud providers such as Amazon EC2) is so easy to set up.

Effective commercial management is a necessity for the successful delivery of any IT programme. In its broadest sense, it can involve all aspects of commercial relationship management - from sourcing and procurement through drafting and negotiating contracts and service delivery agreements, to ongoing service delivery and management.

Commercial management is a specialist skill that requires an in-depth understanding of the business and its aims and objectives, as well as the technology requirements the organisation is trying to address.

All too often, however, organisations rely on supplier-led contracts and the people who are brought in to lead contract negotiations are either whoever is least busy internally (rarely the person with the requisite skills required) or people from outside the business (with little knowledge of the organisation's underlying business requirements) For example, these might include:

- Procurement staff experienced in high volume commodity purchases and unaccustomed to commercial transactions of such complexity. Such resources tend to focus on the bottom line price without conducting a more holistic value for money assessment in respect of the full contract life cycle and/or or the wider organisational benefits/issues.

- Legal advisors who can advise on legal and contract issues but do not have the requisite business or IT context.

In this scenario, data security realities in the Cloud are rarely considered as the relevant stakeholders will not have been consulted. The implications of this are clear - taking the commercial elements of an approach to Cloud Computing lightly could be a serious mistake for any organisation.

In common with any major IT service agreement, proper due diligence at the outset is one of the most important ways of reducing overall risk and users should be careful to note a supplier`s track record, resources, dependence on key sub-contractors and reputation for data/information security.

3. It's your data and your business

Suppliers make it so easy to buy – but there are many hidden dangers. It's easy to swallow blithe claims made by suppliers without bearing in mind the necessary checks that could come back to haunt you in the long run. You need to take commercial arrangements seriously, and put the right safeguards in place.

For example, one lawyer recently explained how one of his clients was using a vendor that said it was certified under the EU and US 'Safe Harbour' legislation which broadly says that the privacy of personal data is protected. However, it turned out that their accreditation under 'Safe Harbour' had lapsed and what they were telling their potential customers wasn't accurate. The lesson from this is that organisations need to verify that what their vendors tell them is true.

Trust must be a watchword – but you have to go beyond trust and back your Cloud venture up with effective service level agreements and legal certainty. At the same time, as regular readers of DAV features will recognise, contracts must be structured and managed to drive behaviour across all parties to achieve the business objectives you require.

Evaluating SLAs can be uncomfortable for many CIOs; after all, most SLAs offered by service providers are constructed against metrics that are correspondingly easy for them to measure and deliver against. They typically take little or no account of the customer's business imperatives. Often the siren attraction of cost savings and easy access to on-tap computing resources offered by the Cloud, causes customers to overlook their normal good practice when it comes to contracting for external services. For example, in their keenness to embrace Cloud Computing to gain perceived business advantage, some organisations may make critical errors that can compromise the safety and security of their data. Additionally, many organisations may sign up to inadequate service level agreements, which introduce new risks to the operational effectiveness of the business.

You have to know where the data is in the Cloud. It's your data and your business is reliant on it. Lose the data – and you could lose part of your business. Potential solutions involve segmenting your data depending on how valuable it is to your organisation – i.e. not putting your most valuable data in the cloud – or, where sensitivity is less of an issue, tag the data or incorporate a tracking mechanism (more commonly known as a 'honey token') that will provide an alert where data is accessed via an unauthorised party. In addition, most organisations are bound by regulatory compliance or customer contracts that place an obligation on them to ensure that data security and confidentiality is not breached or compromised in any way.

Needless to say, the penalties if such a breach were to occur would be severe and this, typically, represent a risk that any business ignores at its peril.

4. Assuring commercial certainty by asking the right questions

How do you gain assurance of commercial certainty in the Cloud? By going into it with your eyes open, approaching Cloud Computing deliberately and by knowing the right questions to ask. This is so important the Information Commissioner's office has even produced some guideline questions to be asked about the security and privacy of data as part of a risk analysis exercise.

These include:

- Ask your vendor to confirm in writing what safeguards it will put in place to ensure that the service provider will only process data in accordance with your instructions and will maintain the required level of security?
- To what extent can the service provider guarantee the reliability and training of its staff, wherever they are based? What form of professional accreditation does it hold?
- What capacity does it have for recovering from a serious technical or procedural failure and what are the documented processes covering this?
- What is its policy for dealing with complaints and providing redress – what compensation does the service provider offer for the loss of data entrusted to it?

- If it is an established service provider, what evidence of its security track record can be provided? What safeguards can be provided by a new entrant to give confidence that security of data will be adequately addressed.

- What assurances can it offer and what safeguards are in place to ensure that data protection standards will be maintained, even if the data is stored in a country with weak, or no, data protection law, or where government data interception powers are strong and lacking safeguards

- Mandating that the service provider will send you copies of your data regularly, in an agreed format and structure so you hold useable copies of vital information at all times?

If warning bells are not already going off, it should be clear from the tone of these questions that Cloud is easy to set up, easy to get wrong and difficult to put right. To ensure you can interpret the answers to these questions, you are going to need an experienced head telling you what you need to know about the commercial requirements, which must necessarily cover data protection and confidentiality, business continuity and service availability and cost.

According to the law firm Clarkslegal, data protection and confidentiality is still the single biggest barrier to a more widespread uptake of Cloud Computing services by the business sector, as businesses are naturally reluctant to entrust key personal, client and/or company data to suppliers where more and more data is held from multiple businesses in different jurisdictions. In addition, given the strict data protection regime in force in the European Economic Area (EEA), the fact that it is sometimes hard to pin down exactly where personal data has been transferred in a Cloud Computing context only increases the challenge of complying with data protection rules and, in particular, the restrictions on the export of personal data outside the EEA. Users need to be checking that suppliers undertake not to export personal data outside the EEA or agree to robust terms consistent with data protection law.

When it comes to business continuity and availability of services, there are a number of different technologies and standards which run the risk of Cloud based solutions not being fully interoperable with legacy services retained in-house, services provided by traditional IT suppliers or services provided by other Cloud Computing providers.

In respect of Cloud-based service charges, it is important for the customer to understand the basis of such charges. Typical questions that will require answers from a service provider are around charging structure, viz:

- what is included or excluded, whether explicitly or by implication
- whether charges are based upon traffic, usage or storage limits
- whether there is any type of price protection
- whether there are licensing fees above and beyond the service fees, or indeed, additional taxes or external fees.

Another key area is suppliers` standard terms and limitations on liability. In general, the leading Cloud Computing providers have adopted standard terms which are not user friendly and contain strict limitations of liability in areas such as service failure and loss of data. There is also a marked reluctance to provide express service level agreements or to share a reasonable element of risk in the event that business critical functions of a user are jeopardised. Issues to consider include: the ability to reduce user numbers/terminate early; obligations relating to keeping data secure; reasonable service levels and post-termination assistance. In keeping with all commercial contracts, the extent to which suppliers are willing to amend their standard terms will depend directly on the size and value of a user`s potential business with it. As the mantra goes, "if you don`t ask..."

Finally, termination and exit provisions are critical. Businesses contemplating entering into a Cloud Computing contract must be assured – and indeed, guarantee - that there is an exit plan with clear terms dealing with the rights and obligations of the parties on termination and in particular, issues surrounding what happens to a user`s data, how and how long it will take the supplier to deliver it and any general obligations on the supplier to assist the user in receiving data back or transferring to a successor supplier.

5. Using a trusted partner to limit your exposure

The harsh reality is that there must be a commercial argument which states clearly what all parties will get out of the arrangement and what parties will do if things go wrong. Getting into Cloud is easy – it can even be done by the business without the IT department being involved, but those who go into it naively can get 'stitched up' and left exposed.

In the past many suppliers may have experienced a very relaxed arrangement with their customers. However, this is no longer the case, all contracts are under the microscope – and this must be especially the case with Cloud Computing.

At the same time, and this is something DAV Management has wide experience of, success is about getting the contract balance right.

Questions customers should be asking themselves ahead of any engagement with a Cloud service provider should definitely include: the certainties of the contract and the deliverables – notably the key issues mentioned earlier such as security of data, business continuity, and cost, while also looking more holistically at the wider commercial agreement. IP infringement, indemnities, liabilities, etc, all need to be hammered out in the context of the service and underlying agreement you are looking to put in place. But perhaps more significantly you need to be clear about the levels of service and business continuity your business needs and what you expect the service provider to sign up to – the what, when and how are critically important here, surpassed only by the remedies you put in place to protect you if things don't happen the way they should and your provider fails to meet the service level agreement committed to.

Answers to the above questions will help determine whether an organisation is able to take advantage of a commodity priced, but potentially less secure Cloud-based service, or whether there is a need to opt for a more secure service provision, either by segmenting certain data or moving towards the other end of the spectrum with a private Cloud. Clearly customers need to recognise the correlation between the type of Cloud service being sought and the associated terms and charges.

When moving away from commodity type services, customers should be very prescriptive about service levels, and they should approach these with the same mind-set and due diligence as a traditional outsourced service level agreement. Experienced external help can be invaluable here to ensure you get an agreement that provides the basis for a successful, long term relationship with your chosen service provider.

The rise of Cloud Computing has necessitated the development of new kinds of provisions to protect the legal rights of both vendors and users. While traditional outsourcing and software licensing agreements can be used as a model, the unique nature of Cloud Computing means contracts must address several new areas of legal liability and risk. As with any service agreement, it is incumbent upon all parties involved to ensure the contractual basis agreed fully represents their interests and provides them with the protections they require.

Similar issues to what we have seen before in the outsourcing revolution will apply in the Cloud, and here there is no substitute for hard-won business experience. If you are wrestling with a complex business change programme or major contract negotiation, you will need someone at the helm with the requisite levels of skill and experience to help secure the outcome that the business needs, a trusted partner who has seen commercial management at the coalface and who can equally apply that experience to help add value to organisations looking to implement evolving Cloud services.

There is no mistaking the potential that this new paradigm offers organisations in all its various guises. But before you leap into the Cloud, if you can't see where you're going, it's worth taking some advice to know what you'll find when you land. As one recent commentary aptly suggested, 'Cloud Computing – stormy weather ahead.'