fieldfisher

Priorities for customers taking cloud services

Introduction

Cloud services vary enormously, with different service models, (Software-, Platform- and Infrastructure- as a Service) and deployments (public, private and hybrid clouds). Different models raise slightly different legal and regulatory issues for customers, but there are common themes. A particular challenge for customers is that, certainly in the public cloud sphere, vendors are offering a commodity service and so offer commodity, non-tailored, (and sometimes non-negotiable) terms to match. However, in our experience, vendors are often willing to negotiate to win big accounts. For smaller customers with less bargaining muscle, the following top ten should provide a checklist of key issues for due diligence.

Security: Do your due diligence

Data security is naturally high on the list of customer concerns. The customer is dependent on the vendor for the security of the service. Security breaches can lead to customer loss - financial and reputational - public censure and regulatory sanctions; but the customer might struggle to obtain suitable security warranties and/or assurances. Customer due diligence can be hampered by a lack of vendor transparency. How will the customer's data be protected? What access controls are in place? What training is provided to the vendor's staff? Does the vendor hold recognised security accreditations? The nature of cloud services means that it might not be feasible to physically inspect the vendor's data centres. Alternatively, the vendor could commission a security audit from an independent third party that could then be made available to customers.

Ideally, the cloud contract should include an incident response plan, a right for the customer to terminate in the event of a security breach, and an obligation on the service provider to notify the customer of any data security breaches.

Check the vendor's service levels and customer remedies for service failures

Even the largest vendors are not immune to service outages. Before committing business critical applications or data to the cloud, customers should press vendors to commit to a credible SLA with appropriate metrics, measurement periods, reporting obligations and remedies for service failures. It is common for vendor contracts to contain wide disclaimers and exclusions of liability. The customer should assess the potential risks of using the service as well as the type and scale of loss that the customer could suffer from a service failure or outage (as it would for any type of technology services contract). Do the vendor's terms allocate a fair proportion of risk to the vendor and/or provide a meaningful incentive for the vendor to meet the agreed service levels?

Plan for an easy exit

A quick exit might be necessary for vendor insolvency, material breach or a business continuity event. Whatever the circumstances, the customer will want to ensure that it can retrieve its applications and data from the vendor's cloud and use and/or transfer them to a replacement service provider. The ideal time to plan and agree exit arrangements with the vendor is before contract signature. Ideally, the contract should include a requirement for the vendor to provide periodic drops of customer data to the customer and/or to return customer data at the customer's request. It should also specify the format in which customer data will be returned (one that is readily useable by the customer) and make appropriate provision for back-up arrangements and migration assistance.

The cloud contract should also address ownership of customer data. This is particularly important because in a virtual environment, there might not be a physical copy of the customer's data and applicable local laws on ownership of intangible data may not be sufficiently clear or developed to enable swift retrieval from the vendor. Check that the vendor's terms do not allow the vendor to delete customer data (for example on termination or on breach of the vendor's Acceptable Use Policy), and if they do, insist that the vendor gives reasonable notice and an opportunity for the customer remedy the default, and that the vendor delivers up copies of the customer data to the customer before data is deleted.

Vendor solvency: do your homework, but plan for the worst

The high profile collapse of UK data centre operator, 2e2, earlier this year shows how important it is for due diligence to extend to the vendor's financial health. Once the administrators move in, it may be too late to secure the migration assistance that the customer needs. It was reported across the technology press that 2e2's administrators told customers that it could take as long as 16 weeks to return their data to them. Worse, customers would have to pay additional fees to enable the data centre to continue to operate while the administrators sought a buyer. If customers were not willing to provide the additional funding, then 2e2's data centres would have to close.

So, what can cloud customers do to protect themselves against vendor insolvency and minimise business continuity risk? Financial distress provisions – if the customer can persuade the vendor to include them in the contract – can give the customer early warning of financial troubles. Vendors are unlikely to resist allowing the customer the right to terminate on the appointment of an insolvency office holder; but, customers might consider trying to secure the right to terminate earlier if there are signs of material financial distress.

Regulatory compliance

Many companies - particularly those in highly regulated sectors such as financial services – must comply with laws that require them to run a robust IT infrastructure for all or the regulated part of their business. This can present challenges in the cloud

context:

- A lack of transparency from some vendors can make it difficult for customers to assess the adequacy of the vendor's security provision.
- The customer's regulator may demand a degree of oversight of outsourced services (for example, through audits) or segregation of the customer data from other data. If so, then it's unlikely that a public cloud solution will be able to satisfy these requirements. Private or hybrid clouds offer a way forward by allowing data and/or applications from the regulated part of the customer's business to be stored on local hardware.

Check the vendor's AUP and consequences of breach

Customers must usually observe the vendor's Acceptable Use Policy (AUP). The vendor might reserve the right to suspend the cloud services and/or to remove offending data for AUP breaches. In the European Union, vendors will usually insist on the right to remove data as part of their "notice-and-take-action" process so that the vendor can benefit from a defence that shields intermediaries ("hosts" and "mere conduits") from liability for third party content. Customers, in turn, will want to ensure that the AUP includes a reasonable process for handling illegal content and gives the customer a reasonable opportunity to remedy AUP breaches before triggering termination.

Avoid lock-in

To avoid lock-in to a particular cloud vendor, customers must be able to migrate their data and applications, whether back in-house or to a new cloud provider or data centre. There is a growing market in open cloud solutions and solutions based on open standards, as vendors recognise that interoperability and portability are key customer concerns.

Is the vendor signed up to SaaS Escrow arrangements?

A number of escrow service providers now offer cloud business continuity solutions including:

- "Recovery as a Service" – where the escrow agent maintains a complete recovery environment that mirrors the vendor's cloud infrastructure and the customer's data. The recovery environment is made "live" and available for the customer's use for a limited period after the occurrence of pre-agreed trigger events, to allow the customer time to make alternative arrangements;
- Escrow/deposit of all source code, infrastructure information and data necessary to enable the customer to recreate the vendor's cloud environment, with provisions for the release of that material to the customer on pre-agreed trigger events.

Migrating applications to the cloud: check your licence terms

Customers should check their software licence terms carefully before migrating existing applications to the cloud. It's essential that the licence terms permit transfer to a cloud platform, but also that the customer's planned use is in line with any restrictions in the licence, such as territory, number and location of users.

Personal data and privacy

Getting privacy right in the cloud is vital. European privacy rules require customers to place contractual controls on how their service providers handle personal data and restrict exports of personal data to countries outside of the European Economic Area. The Article 29 Working Party (the body of European privacy regulators) has set the bar high on compliance. Its highly prescriptive approach includes some 14 recommended contractual obligations and assurances that cloud customers should seek from vendors. For businesses affected by European privacy rules, the restrictions on international transfers can be a challenge. Customers may not have visibility of where their data is being processed, particularly if the vendor's cloud infrastructure is dispersed across a number of data centres in different jurisdictions. Going forward, Binding Safe Processor Rules will be an important means for legitimising international transfers of personal data. These intra-group arrangements allow cloud vendors to satisfy their customers that the vendor will process the customer's personal data in a privacy-compliant way, and importantly, will be recognised by European privacy regulators.

Conclusion:

The cloud offers customers innovative, flexible, scalable solutions for low up-front costs and utility-based or recurring fees. Nonetheless, widespread adoption continues to be hampered by customer concerns over some of the issues highlighted in this top ten. We advise our clients to engage with the vendor over any concerns. If the vendor is unwilling or unable to offer the comfort (contractual or otherwise) that the customer requires, then at least the engagement process will have flushed that out, allowing the customer to make an informed decision whether to proceed or find an alternative solution.

Contacts

Phil Lee
Partner - Palo Alto

E: phil.lee@fieldfisher.com
T: +1(650) 513 2769

Mark Webber
Partner - Palo Alto

E: mark.webber@fieldfisher.com
T: +1 (650) 513 2684