KPMG

Moving to the cloud – key considerations

Key risk considerations for decision makers

—

February 2016

Executive summary

Cloud computing is an established and trusted model for the delivery of IT services in both the public and private sectors. Indeed, cloud should now be the default option considered by public sector buyers of IT products and services as stated in the Cabinet Office principle of "Cloud First". Similar "Cloud First" principles are also being rapidly adopted by the private sector; we see a variety of FTSE 250 clients looking to move to a predominantly cloud-based IT delivery model over the next 24 months. Organisations now have confidence that Cloud offers the cost-effectiveness, agility and security necessary to support the on-going digital transformation common across both public and private sectors.

Nevertheless, there remains a lack of awareness of the nature (and associated risks) of cloud computing within senior decision makers within enterprises which can inhibit appropriate adoption of cloud services, potentially jeopardising future competitiveness.

This paper outlines the key features and risks of the various forms of cloud computing and provides decision makers with the set of key issues to address when considering the adoption of cloud services. These key issues are shown below:

Organisations following this approach should find themselves in a position to be able to operate in a "Cloud First" manner and, more importantly, able to make the most of the undoubted benefits that cloud adoption can offer, cognizant of any relevant considerations to their organisation, in terms of cost-effective agile IT delivery.

KPMG

Contents

Introduction

This paper is a short guide for decision makers who are accountable for information risk, and other senior individuals who need to make appropriate, proportionate and risk-aware choices when considering the purchase of cloud computing services for enterprise use.

Cloud computing is a market that is evolving and expanding rapidly. When thinking about cloud computing there are many non-functional dimensions which should be taken into account, including data protection, data security and data sovereignty. These considerations apply to any form of technology service, but can become more complex in cloud, where the cloud platform may be shared with many other unknown tenants and where customer data may be stored and processed in many different jurisdictions.

Despite these complexities, the benefits of cloud can be immense, as cloud can enable organisations to deliver business outcomes and innovation quickly, securely and sustainably with little, if any capital expenditure. There are many different kinds of cloud services, and many different kinds of cloud service providers. This paper helps decision makers choose the right cloud service and service provider for the job, in order to get the optimum benefits from cloud, without compromising the overall security of information assets.

KPMG

The perfect storm: Cloud in the UK

Cloud computing is not new

As personal consumers most of us have been using cloud for years, even if we were not aware of the fact, services such as Hotmail (now Outlook.com), Netflix and Skype are all provided from "the cloud". What is new, is that cloud is now increasingly being adopted by enterprises keen to exploit cloud's many advantages. Cloud comes in many shapes and forms, from shared applications used to manage your HR processes or sales teams through to the capability to build your own virtual infrastructures on shared physical hardware and myriad forms in-between.

Enterprises initially displayed a great deal of cynicism about control over their data and services. This "not invented here" mentality is slowly receding, however we do still meet Chief Information Officer's (CIOs) who see cloud as a threat to their influence and so whom point to poorly defined security concerns as a reason to delay implementation of cloud-based services.

Another of the barriers often quoted by those reluctant to adopt cloud services relates to compliance requirements. However, guidance issued by the Information Commissioner's Office[1] and (proposed) guidance issued by the Financial Conduct Authority[2] make it clear that there are no fundamental reasons why enterprises cannot adopt cloud from the perspectives of those two high-profile authorities. That is not to say that there are no compliance concerns, simply that they require managing alongside other issues rather than being used to prevent progress.

For every argument against cloud adoption, there is a counter-argument for cloud adoption, supported by cloud services and cloud service providers that demonstrate that the cloud model has the maturity, breadth and experience to meet the often very diverse needs of the market. Cloud services are particularly well-suited to meet the needs of the more agile project and operations delivery methodologies being adopted throughout industry.

The efforts of many cloud providers to be transparent about their operations (including obtaining independent assurance certifications) and the increasing number of success stories has steadily eroded the arguments of those resistant to the adoption of the cloud model. Many governments, including the US and the UK, are now actively transitioning to cloud whilst innovative companies across many industries are challenging established players thanks to the agility offered by their chosen cloud providers. Cloud is not just for the challengers – we do also see some large organisations (including members of the FTSE250) making the wholesale leap into the cloud, with some looking to be able to close their own physical datacentres within a couple of years.

However, for over twenty years 'UK Plc' has operated its legacy technology provisioning through a mixed economy of IT Outsourcing, Business Process Outsourcing and, typically in the larger enterprises, in-house provision. Where IT services have been externally sourced, the commercial characteristics have

[1] https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[2] https://www.fca.org.uk/news/guidance-consultations/gc15-06-proposed-guidance-firms-outsourcing-cloud

tended towards expensive, long term and difficult to break contracts, held with a small, elite group of service providers. This has left many organisations with a skills gap in their retained IT function and overly reliant upon their systems integration partners.

Cloud offers organisations an alternative model, where IT services are generally sold on a commodity basis. A consuming organisation may only pay for what they use, when they use it, making cloud a highly cost effective model, compared to legacy systems, which are normally built and priced to cope with peak demand. Typically, a consumer can buy cloud services without capital expenditure, as they are effectively leasing part of a cloud providers pre-existing infrastructure. Many cloud providers do not penalise consumers if they cease to consume, or leave their services. As such, cloud services have been key to the current digital transformation within organisations across many different sectors; cloud is ideally suited to support and enable agile project delivery methodologies.

Cloud Adoption - key risks and how to mitigate them

Transitioning to the cloud is a non-trivial decision for most organisations, and those responsible and accountable for making such a decision must evaluate the data and service(s) that they plan to migrate to the cloud. Questions to consider include:

Key risks

- How sensitive is the data, and what are the necessary minimum security controls?
- How critical is the service to the organisation, its partners and its customers?
- Is the data subject to regulation?
- Do privacy restrictions apply?

Operational risks

- How is the confidentiality, integrity and availability of data maintained?
- Where is the data stored?
- If the data is stored off-shore, are the additional legal implications and risks assessed and understood?
- Can the data be encrypted in transit and/or at rest?
- Who generates, holds and distributes the encryption keys?
- Where is the data encrypted?
- How can you monitor what happens to your data over a diverse cloud-based supply chain?
- How can you make your users access to cloud services seamless yet secure?
- What independently assured certifications and accreditations does the cloud provider hold?
- Where are the cloud providers service centres, and what level of vetting have their staff undergone?
- Can the data and service be easily moved to another provider?
- Does the provider preclude you from conducting your own penetration testing of your own services?
- Is the provider and service compliant with applicable regulation?
- What jurisdiction is specified within the contract for the purposes of conflict resolution?
- Is the cloud contract fit for purpose and compliant with all applicable regulation?

KPMG

Cloud definitions and security implications

Many definitions relating to cloud computing have been published over the past few years, however the de-facto standard, is that of the US National Institute of Standards and Technology (NIST).

The NIST document[3] defines a set of essential cloud characteristics, three service models (the well-known terms of Infrastructure as a Service, Platform as a Service and Software as a Service) and four deployment models (Public, Private, Community and Hybrid). The NIST definitions are shown at Annex A.

Cloud Service Models

— Infrastructure as a Service (IaaS) – IaaS generally allows users to provision a virtual infrastructure for the processing and storage of data. Consumers can deploy a variety of virtualised servers in a flexible and easily changed configuration.

— The cloud provider is responsible for the security of the underlying physical hardware and the data centre(s) hosting the service. However, the consumer, or a third party on behalf of the consumer, is responsible for configuring and operating the guest Operating System, software, and virtual networking between the virtual servers, including external connectivity such as to and from the Internet or to legacy data centres or office locations.

— Consumers remain responsible for maintaining the security of their virtualised servers in terms of the application of security patches, use of anti-virus solutions and other traditional operational security controls, as with more traditional on-premises infrastructures.

— The consuming organisation takes on the operational risk that exists above the shared physical infrastructure level, from the operating system and virtual networking upwards.

— The onus is therefore on the data and service owners to evaluate the nature of the data and services that they propose to migrate to the cloud, to understand the security controls that are needed to protect the data, and to be satisfied that the cloud provider has these controls.

— These controls include, but are not limited to; logical and physical access controls, the ability to perform IT Health Check (ITHC) tests to identify any vulnerabilities, compliance activities such as ISO27001 certification or production of ISAE3402 SOC2 reports, as well as regulatory and legislative compliance, and the following of industry good practice, e.g. alignment with the Cloud Security Alliance Cloud Controls Matrix[4].

— Many providers dedicate sections of their web-site to the provision of information relating to security and assurance status, and some will be able to provide independent verification of its security controls. Public sector organisations should also look to check alignment with the 14 Cloud Security Principles[5] issued by CESG and evaluate the self-asserted security claims made by G-Cloud providers or, better still, seek independent verification of

[3] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[4] https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[5] https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

the provider claims. Private sector organisations can also gain insight into the security posture of potential cloud providers through examination of the provider's entry on the G-Cloud web-site[6].

- Data owners retain many more operational security responsibilities in the IaaS model than with the other cloud service models (PaaS and SaaS) due to the need to secure their own virtualised servers and networks.
- With IaaS, the boundary between the different customers of the provider, i.e. between one consumer and another, is typically the hypervisor – the management layer that allocates physical resources to the virtual servers. In other words, consumers can find themselves sharing a physical server with other customers of the cloud provider. Some IaaS cloud providers will offer dedicated instances whereby they commit to not sharing a physical server with other customers for an additional fee.
- Platform as a Service (PaaS) – PaaS provides consumers with the ability to develop and deploy applications of their own choosing on to a pre-configured "platform". In essence this means that the providers are responsible for the security and maintenance of the underlying virtualised infrastructures that provide the platform.
- In contrast to the IaaS model, PaaS providers are responsible for server/operating system security issues, which allows PaaS consumers to concentrate on application level security concerns. PaaS offers an efficient and agile approach to deploy, operate and scale-out applications in a predictable and cost-effective manner.
- Service levels and operational risks are shared because the consumer must take responsibility for the stability, security and overall operations of the application while the provider delivers the platform capability (including the infrastructure and operational functions) at a predictable service level and cost. PaaS takes away the inconvenience of managing operating systems and allows organisations to focus on the higher business value areas of application development and operation where more of the User Needs are evident.
- As well as considering the risks listed above with respect to IaaS, PaaS data and service owners must satisfy themselves that the PaaS product does not have inherent vulnerabilities which could lead to either data breach, or the introduction of malicious software. PaaS providers should be able to provide clear policies, guidelines, and standards, and conform to industry accepted best practices.
- Due to the less-defined nature of PaaS, consumers need to be particularly careful about the distribution of security responsibilities between themselves and the provider as the handover points can be harder to define than with the IaaS and SaaS models. With PaaS, consumers are still responsible for the development of the security-relevant aspects of the application, for example identity and access management, security logging and application level security testing (penetration testing).
- The boundary between different customers in a PaaS is dependent upon the specific PaaS provider – some may use formal containers (e.g. Docker, rkt) to separate different applications running on the platform, others may take a more custom sand-boxed approach. With PaaS, consumers could find themselves sharing an operating system instance with other customers of the Provider.

[6] https://www.digitalmarketplace.service.gov.uk/g-cloud

— Software as a Service (SaaS) – Software as a Service (SaaS) delivers business applications for a usage or subscription-based cost at an agreed service level. In other words, consumers can make use of a shared service, such as a Finance application or E-mail service (for example), which removes any requirement for the consumer to develop and secure its own application and infrastructure (although a level of configuration effort will likely be required).

— SaaS can provide significant efficiencies in cost and delivery in exchange for minimal customization opportunities. Consumers are no longer responsible for the security of the application itself, but do remain responsible for the secure usage of such applications. The SaaS approach is therefore well-suited to those areas of business where little competitive advantage can be achieved through differentiation, e.g. human resources.

— In addition to the service risks applicable to all cloud services, consumer of SaaS services need to have a clear understanding of application-level risk, for example taking into account how the application handles authentication and authorisation, user access provisioning and security monitoring.

— Consumers should also assure themselves of the adequacy of the security testing and development practices of the SaaS provider to address issues such as configuration, content-filtering and session management vulnerabilities.

— With Software as a Service, the boundary between customers of the provider may sit within the application itself, i.e. different customers may be accessing the same application instance with the separation between clients being reliant upon the access controls within the application itself.

Cloud deployment models

The NIST model defines four cloud deployment models, each of which are described as follows:

— Private Cloud – With a private cloud, organisations build their own dedicated cloud infrastructure. This dedicated infrastructure could be procured, built and managed by the organisation or it could be provided to the organisation by a third party – either on-site or in a remote data centre. The advantage of private cloud infrastructures is that they can be more straightforward to secure due to the lack of multi-tenancy, i.e. no other customers of a cloud provider have access to the dedicated equipment.

— The disadvantage of private clouds is that they can be slow to deploy (due to traditional procurement and implementation timescales if building in-house), and expensive, as few cloud service providers would be willing to meet the cost of the capital expenditure on the basis of a pay as you go provisioning model.

— A private cloud implementation may therefore require significant capital expenditure in the form of Set-Up costs; organisations lose many of the benefits often desired from the shift towards operational expenditure seen with public cloud, and may not enjoy the constant price reductions currently associated with public cloud.

— Those organisations building and running their own private clouds do not benefit from the "illusion of infinite resource" that is offered by the public cloud – such organisations must continue to procure sufficient hardware to meet peaks in demand. Similarly those organisations hosting their own private clouds must still invest in their own physical data centres, including resilience and fail-over capabilities, which limits their availability options in comparison to the major cloud providers.

- Community Cloud – Organisations can reap many benefits from working together through a community cloud strategy. The shared service model is well established within many sectors, and the development of community clouds based on organisational families with common standards, security needs and regulatory constraints is a logical extension.
- Community clouds can be thought of as a halfway house between the private and public cloud models, for example some of the scalability and resource constraints of a pure private cloud may be less of an issue in the community model.
- This may not however be the case for those communities which are likely to have peak demand at the same time, e.g. the Police service in the event of a national incident. In which case, such a Police community cloud would either still need to be sized to meet peak demand or else be rapidly scalable to meet short-term spikes in demand.
- Consumers are well-advised to consult with their potential community cloud providers to ascertain the scalability and elasticity of their solutions; not all community cloud providers are created equal.
- Public Cloud – A public cloud service provider makes available applications, data storage capacity and other resources to organisations or the general public using its own servers. Public clouds offer all the advantages of rapid service deployment, and utility pricing. Public clouds can also be very secure, and in many cases do not operate on a global, or even cross border basis, i.e. they are based within a single nation.
- Hybrid Cloud – Hybrid cloud balances the use of different cloud deployment models and can offer organisations the advantage of flexibility and scalability. Hybrid cloud allows organisations to balance isolation, cost and scaling requirements.
- An example would be the ability to deploy services internally when internal capacity is available, but moved to the public cloud services when it is unavailable. Other examples may include the use of public cloud for the storage of data back-ups or to provide a disaster recovery capability without the expense of building multiple geographically separated data centres.
- One potentially worthwhile deployment option is to build a private cloud containing certain central security services, e.g. identity and access management controls, which are then used to secure assets hosted in public, or community, clouds.
- Hybrid cloud may be an interim option where an organisation has legacy or interdependent services that cannot be trivially decoupled and moved to a public cloud
- From a security perspective, the hybrid cloud approach requires the consumer data owner to consider the security issues associated with all elements of their solution, e.g. both the issues relating to private cloud and the issues relating to public cloud if the hybrid solution is to be used for bursting to the cloud in times of high demand.

One obvious consideration about the hybrid model, which is often missed, is this: if data is suitable to go to the public cloud at times of peak demand, why not just operate in the public cloud at all times? There may be some situations whereby it's more cost-effective to operate in on-premises data centres (e.g. 24x7 operation, constant demand) and burst out if you run out of resource. Typically however, the hybrid model is often used as a stepping stone towards full adoption of the public cloud model once any remaining reservations or concerns have been addressed through experience.

Cloud Service Providers

The global cloud marketplace is evolving and expanding at a very rapid rate. The Cisco Global Cloud Index Forecast, 2013 – 2018[7], makes the following forecasts:

— Global data centre traffic will nearly triple from 2012 to 2018.
— By 2018, global data centre traffic will reach 8.6 zettabytes per year.
— By 2018, more than three quarters (78 percent) of workloads will be processed by cloud data centres.
— By 2018, 31 percent of the cloud workloads will be in public cloud data centres, up from 22 percent in 2013.

Cloud is an industry which is expected to grow in line with exponential data growth, which in itself is simply symptomatic of other technology developments such as the continuing development of the Internet of Things and the maturing of data analytics. Together with factors such as user convenience, speed of deployment, ease of operations (infrastructure as code), closeness to end users (via the Internet) and the improved competitiveness of those adopting cloud, the market is unlikely to slow down in the near term. As such, more and more cloud providers are entering the market. Cloud providers can be categorised in many ways:

IaaS providers specialising in IaaS compute and storage, providing a platform for others to build and operate applications.

PaaS providers that provide a software development platform, where developers can implement software services without needing to be concerned about the underlying infrastructure.

SaaS providers that supply pre-built applications running in the cloud.

Cloud Service Brokers are organisations that aggregate a number of different cloud services in order to provide a single business service to their clients. For example, a cloud service broker may offer a customer relationship management (CRM) service to a consumer – this CRM service may itself be composed of a multitude of cloud services that are invisible to the end consumer.

Cloud Exchanges are organisations that maintain direct connectivity between a variety of cloud platforms and so enable easier portability of services and the ability to host services across multiple cloud providers. Such Cloud Exchanges also enable their customers to develop cross cloud services that do not require the data to traverse the Internet.

Internet Service Providers (or cloud platform providers) provisionally defined by the European Commission as "software-based facilities offering two- or even multisided markets where providers and users of content, goods and services can meet", with examples including internet search engines, social media, knowledge and video sharing websites, news aggregators, app stores and payment systems. Some cloud providers supply IaaS,

[7] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html http://www.bbc.co.uk/news/technology-34185575.

PaaS and SaaS, or indeed a combination of the different services.

Global public cloud providers, like other cloud providers, may allow their consumers to benefit from economies of scale, scalability, and generally a greener and more sustainable model than for legacy IT. This type of cloud computing model offers many benefits, but can have a number of inherent challenges, where consumers may:

— not know where their data is, and will therefore not be able to gauge the level of risk from exposure to foreign jurisdiction (although most major providers do let you set a specific geographic region to host your data and service but the granularity of that control may vary, e.g. Western Europe may mean data centres located in Ireland and the Netherlands. In other words, your data may still be subject to multiple jurisdictions)

— have concerns that the cloud provider has an open back door to its home national security services

— have concerns that by using global cloud providers they are increasing the risk of breaching UK and European data protection regulation, even if they host services in Europe

— have concerns that the cloud provider will undertake unlawful secondary data processing

— not know who their neighbours are in a multi-tenant environment which could, in theory, result in side-channel attacks whereby their neighbours may extract information such as encryption keys

— be subject to standard, non-negotiable contract terms and conditions which offer little, if any redress for service failure, damage to or loss of data

— wish to avoid the reputational damage associated with doing business with a cloud provider who may be perceived as engaging in systemic tax avoidance and adding little if any value to local or national economy

— be concerned that they will be locked in to a cloud provider, where it could be costly and very difficult to transfer data to another provider should the need arise – this risk should be considered in comparison to lock-in in a traditional outsourcing arrangement.

However, cloud providers are evolving as the cloud market place matures to address the concerns typically associated with the global cloud service providers. Some cloud providers:

— may enable data to be processed and stored on-premises, only in one country, or in a limited range of jurisdictions, such as the EU, therefore limiting or even eliminating the risk of foreign surveillance (subject to local exemptions for national security) or breaching regulation

— are now specialising in providing highly secure services, where the level of security is independently verified through certification or accreditation

— are developing privacy policies and terms and conditions which either expressly exclude the possibility of secondary data processing, or which require the consumer to expressly consent to secondary data processing

— have developed cloud platforms which are exclusive to consumers with common needs, and regulatory requirements – "community clouds"

— design and adapt their services to meet the specific and evolving needs of specific sectors, e.g. the legal profession or the UK public sector

— have developed terms and conditions which are more equitable to the cloud consumer, and which comply with the regulatory requirements of the markets they are addressing

— design their platforms and their contracts to allow easy exit of consumers (and their data), and provide advice to consumers to enable consumers to configure their cloud services in a way which minimises lock-in.

Consumers must satisfy themselves that the cloud provider they choose is capable of fulfilling the consumer's regulatory, legislative and security requirements (within a level of tolerance agreed by the business stakeholders

as part of an overall consideration of risks vs benefits). Many cloud providers comply with global and local standards, and hold externally verified certification to validate this compliance.

There are a number of different assurance options available to cloud service providers including:

- ISO/IEC 27001 – the international standard for Information Security Management Systems (ISMS)
- ISO/IEC 27018 – relating to the protection of Personally Identifiable Information in Public Clouds.
- ISO/IEC 27017 – relating to information security controls in cloud services.
- SSAE16 and ISAE3402 – service assurance reports, tailored to provide independent assurance that security controls are operated in line with the claims of the providers
- Cloud Security Alliance STAR (Security, Trust and Assurance Registry) – an independent assurance that the security controls at the provider are in line with the Cloud Controls Matrix produced by the Cloud Security Alliance.

Independent assurance is critical in the cloud model due to the lack of support by many cloud providers of a customer right to audit. Assurance reports may be the only vehicle available to cloud consumers to inform their decisions on whether or not the cloud provider controls are sufficient to meet their minimum baseline of security requirements.

KPMG

Commercial and Contractual Considerations

Data sovereignty and jurisdiction

Processing data in the cloud is legally complex, no matter where the data is being processed. Whilst applicable law is almost always determined in a contract, the contract may not necessarily be enforceable in part or in full, depending on where the data is being processed and stored.

Data is subject to the laws of the country in which it is stored ("data sovereignty"). However, the data processors and data controllers are subject to the laws of the country in which they received the data from the data subjects. The cloud raises new questions around data sovereignty. Laws from other jurisdictions could apply to the data ("applicable law"), depending on a set of scenarios which are evolving through case law. As the vast majority of existing laws predate the advent of widespread use of the Internet, never mind the more recent proliferation of cloud services, it is likely that there will be much change in legislation in this area over the coming years.

It is possible to have numerous jurisdictions apply to data held in the cloud, and this is particularly the case where the cloud provider is non UK, or has a non UK parent company. A fairly common example would be where a UK organisation wanted to use a cloud service provider with a US parent company, which was hosting data in an Irish data centre:

— Irish law would apply in the event that Irish Police want to issue a search warrant to access data in the Irish datacentre

— US law would apply in the event that a US judge wanted to oblige the US parent company to hand over data from the Irish data centre to the US judge (to be determined by an on-going court case between Microsoft and the US Department of Justice[8])

— Irish law would help determine whether the US court order could be enforced

— English law would apply in determining whether any of the above put the UK organisation in breach of the Data Protection Act (DPA).

This is an area which is still evolving and organisations should therefore keep a watching brief on the legal issues surrounding data sovereignty.

[8] http://www.bbc.co.uk/news/technology-34185575

Commercial considerations

A genuine cloud service is standard, with little – if any – opportunity to bespoke the service (although consumers may have opportunities to choose additional standardised service features, and some SaaS services may require an initial configuration or enable "skinning" of the application to reflect the consumer's own branding). Standardisation allows cloud providers to achieve significant economies of scale which will be passed through to consumers in the form of highly competitive pricing and more stable services.

Therefore, cloud contracts are generally standardised too, with little, if any, scope for negotiation, as it does not make economic sense for a cloud provider to manage non-standard contracts against a standardised service.

Within this context, there are a number of contract types:

Consumer to business: typically these contracts relate to free cloud services, such as Facebook, where the cloud provider makes its money through advertising and/or the secondary processing of customer data. This type of contract has no scope for negotiation, and consumers generally have few rights under the contract.

Business to business: these contracts generally relate to services which an enterprise is paying for. There is usually little scope for negotiation, but the contract will usually vest more rights to the consumer – although the cloud provider's liability for service performance (including data damage and loss) may in some cases be very limited. The contract may also permit the cloud provider to unilaterally modify both the service and the contract, and place technical and contractual constraints on switching from one provider to another. Cloud providers can offer additional contractual terms, e.g. enterprise agreements or adherence to the EU Model Contract Clauses relating to data protection, over and above the default terms.

Bespoke contracts: whilst cloud providers rarely offer scope for negotiation of their contracts, it is not correct to say that there is never any negotiation. Cloud providers have been known to negotiate specific agreements with those consuming organisations viewed as particularly influential or large volume[9].

As with any contract, cloud contracts vary: some are balanced and fair to both parties, whilst others are unbalanced, favouring the cloud provider. Organisations need to take a number of key considerations into account, to ensure their legal and regulatory obligations can be fulfilled, that the jurisdictional implications are understood, that the data in their care is not exposed to unacceptable risk, and that the contract is fair and equitable, giving adequate protection to the consuming organisation should anything go wrong. These considerations are set out in detail at Annex B.

[9]http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199

Privacy Considerations

The UK Data Protection Act 1998 (DPA) applies to cloud in the same way as any other technology where personal data is concerned. The act places specific obligations on data controllers (generally the institution that owns the data) to ensure compliance with the eight principles of the DPA. The seventh principle relating to security of data and the eighth principle relating to the geographical jurisdiction of where data is stored are often problematic for UK organisations considering a move to cloud.

The most common form of data protection breach usually relates to the loss or theft of devices or papers. The Information Commissioners Office publishes regular statistics about the number and nature of the data breaches reported to it[10]. The majority of data breaches are reported by public sector and third sector organisations. Big Brother Watch recently published a report[11] which showed that on average, Local Authorities were committing four data breaches a day, and a substantial number of these breaches concerned human error, and lost or stolen data.

The Information Commissioners Office (ICO) can impose substantial fines of up to £500,000 should data controllers breach the DPA. These fines will increase substantially when the forthcoming EU Data Protection Regulation (GDPR) becomes law in 2016, although there is expected to be a grace period of 24 months before the law is enforced by the national authorities such as the UK ICO. From 2018, those organisations breaching the GDPR may be fined up to a maximum or €20,000,000 (or 4% of global turnover of the previous financial year, whichever is higher) for breaches of certain listed articles[12].

It is widely recognised that processing and storing data in the cloud can make the data controller less susceptible to breaching the DPA (provided the cloud service provider complies with the DPA) in comparison to operating in legacy data centres. Cloud service providers tend to operate within highly secure parameters – physical and virtual – thereby minimising the risk of human error, and data theft and loss. As a further example, data shared via the cloud is usually more secure than data shared via easily lost USB sticks.

Decision makers will want to satisfy themselves that personal data is being processed and stored in accordance with the law, as ultimately the data controller will be accountable (and liable for any sanction by the ICO) in addition to taking the reputational damage relating to negative commentary from the media. This assurance is normally addressed through the contractual agreement between the consuming organisation and the cloud service provider.

In the future, under the GDPR, data processors will be placed under additional requirements and will be fined directly for breaches of their obligations. The GDPR does place additional requirements on the controller (in comparison with the current DPA) but if the controller has taken all the necessary precautions, then it may be we see more processors being fined and suffering the negative media coverage.

[10] https://ico.org.uk/action-weve-taken/data-breach-trends/

[11] http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf

[12] http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

UK Data Protection Act 1998 – the seventh Principle

The seventh data protection principle requires organisations to implement "adequate" technical and organisational measures to protect personal data from unauthorised access, disclosure, loss, damage or destruction (amongst others). Where a cloud provider is being used to process personal data on behalf of an organisation, the organisation as data controller will be legally accountable for what the cloud provider does with the data. This includes being held liable where data stored or processed by a cloud provider is lost or destroyed.

Cyber security (the protection of systems, networks and data in cyberspace) is increasingly important for all organisations. Cyberspace is unregulated and cyber-crime is becoming simpler and cheaper to commit. Therefore decision makers must be satisfied that the cloud provider has adequate measures in place to protect personal data securely against unauthorised or unlawful processing and against accidental loss, destruction and damage, and that the contract between the organisation and cloud provider clearly sets out the respective responsibilities and liabilities of the data processor and the data controller.

UK Data Protection Act 1998 – the eighth principle

Cloud providers typically store and move data around multiple data centres situated in a number of jurisdictions, which in many cases may be outside of the European Economic Area (EEA). Under the DPA, the eighth principle restricts the transfer of personal data outside of the EEA, unless the EU has determined that there is an adequate level of protection in place in relation to the processing and storage of personal data. The Information Commissioner's Office provides extensive guidance on the eighth principle of the DPA[13] and its derogations:

- EU Model Clauses for data protection: many non-EU cloud providers incorporate the EU approved model clauses for data protection within their contracts. These clauses have been approved by the European Commission as an appropriate mechanism for satisfying Principle 8;
- Binding Corporate Rules: Binding Corporate Rules are a set of data protection policies, processes and standards, together with contractual provisions that bind the entities and employees of an international organisation to adhere to them. They solely cover the transfer of personal data to other organisations within the group based outside the EEA. In the UK, Binding Corporate Rules must be authorised by the ICO;
- Other derogations: in some cases it is permissible to transfer personal data out of the EEA even when a lower level of data protection would apply. The derogations include where the data subject has consented to the transfer, although this consent may be withdrawn, or where the transfer is in the public interest. This is not an exhaustive list of the derogations (many of which are not always directly relevant to public sector organisations), however in all cases all other aspects of the DPA apply, and the ICO recommends a narrow interpretation of the derogation provisions;
- Local Adequacy decisions: Local Data Protection Authorities (in the UK this is the Information Commissioner) can make an adequacy decision. This can be time consuming and is rarely used.

[13] https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf.

KPMG

List of Adequate Countries

The European Commission has determined that a limited set of countries do provide adequate protection of personal data to enable the transfer of personal data from the EEA. From a global perspective, this list is highly restricted, with only 11 countries featuring on the list, namely:

— Andorra

— Argentina

— Canada

— Faroe Islands (with certain limitations)

— Guernsey

— Isle of Man

— Israel (with certain limitations)

— Jersey

— New Zealand

— Switzerland

— Uruguay

Anonymisation and Encryption of Personal Data

The Office of the Information Commissioner has issued guidance on the use of anonymisation techniques to take personal data outside of the scope of the data protection act. According to the ICO, truly anonymised data is no longer personal data as it is no longer possible to identify an individual; the exact statement used within the guidance document[14] is,

"Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."

However, true anonymisation of data is a non-trivial problem to solve due to the ability of an attacker to link the anonymised data with other information sources which may result in the subject being re-identified. Numerous examples of the dangers of re-identification have been published in the past, notably relating to data released by AOL[15] and Netflix[16]. Techniques are available to make it mathematically infeasible to identify a specific individual within an anonymised dataset, e.g. differential privacy, however anonymisation, de-identification and re-identification are still emerging and active fields of research. Potential creators of anonymised data should also be aware that just because you cannot identify a specific individual does not mean that you cannot ascertain personal information about an individual, for example where all potential matches to an individual within a dataset share a property previously unknown to the attacker (e.g. a specific illness).

Pseudonymisation is a mechanism to reduce the linkability of a dataset to the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation. The views from regulators is that the following are generally forms of Pseudonymisation:

— Encryption with secret key

— Hash function

— Salted-hash function

— Keyed-hash function with stored key

— Deterministic encryption or keyed-hash function with deletion of the key

— Tokenization

The use of encryption therefore does not take personal data outside of the scope of data protection law since the creator of the pseudonymised data can still identify the individuals contained within the data.

[14] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

[15] https://en.wikipedia.org/wiki/AOL_search_data_leak.

[16]https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

The Future

Data privacy versus national security

As we generate more and more data – all of which needs to be processed and stored – and as we develop more and more capability to exploit data, as often for the good of mankind as for the benefit of industry, so data privacy has become an increasingly high profile and politicised topic. The Snowden revelations have given the privacy rights campaigners a hook to hang their case on, and have deeply damaged Europe's trust in US service provider's ability to comply with European data protection regulation. Of course, the national security services in countries other than the US should not be thought to be any less voracious in their appetite for information – the NSA may have more capability than most but it would be a mistake to limit considerations of threat to a single nation state. Citizen concern over security agency access to their data has led to a number of cloud service providers offering transparency reports which provide approximate numbers of information access requests that they receive from national security agencies. Legislation often prevents the reporting of exact numbers.

The European Commission is investing a great deal of time and effort in regulating so called "platform" providers, such as Facebook and Google, firstly to ensure that European personal data is always treated in compliance with European data protection regulation – irrespective of where that data might be, but also in some cases to address the perceived anti-competitive behaviour of some of the platform providers.

A number of significant initiatives are in play, none of which have reached finalisation, and all of which serve to create a climate of uncertainty in terms of the relationship between data controllers and non-European cloud providers, as there is currently no stable legal framework.

Safe Harbor

The Safe Harbor Agreement was an agreement between the US and the EU, where US companies self-certified that they would process European personal data in compliance with the seven principles of the Safe Harbor framework. The provisions of the Safe Harbor scheme were, until very recently, considered an appropriate mechanism to satisfy Principle 8, thus allowing European companies to transfer personal data to Safe Harbor registered companies in the US without needing the use of EU Model Clauses (or an alternative mechanism).

The Snowden revelations did nothing to instil Europe's confidence in Safe Harbor. In November 2013 the European Commission subjected Safe Harbour to a 13 point plan in an attempt to restore trust in EU-US data flows. By early 2014 the European Parliament had called for the immediate suspension of the agreement. The agreement was then subject to renegotiation by the European Commission and the US, negotations that were given fresh impetus following a court case at the European Court of Justice.

Privacy rights activist Max Schrems had raised a series of complaints against Facebook Ireland with the Irish Data Protection Commissioner (DPC). All of the complaints related to perceived shortcomings in Facebook's privacy practices, including the allegation that Facebook Ireland forwarded data to the NSA. The complaints were refused outright by the Irish DPC, on the grounds that Facebook's Safe Harbor self-certification meant there were no grounds for investigation.

Schrems then filed a judicial review against the Irish DPC's findings which was referred by the High Court of Ireland to the Court of Justice of the European Union, to clarify whether Data Protection Authorities (DPAs) were absolutely bound by a European adequacy decision, or whether they could make their own adequacy decisions.

The court found:

- The Safe Harbor decision was invalid, and the agreement does not afford an adequate level of data protection
- EU DPAs and courts can independently determine whether cross-border data transfer mechanisms comply with EU requirements, regardless of a finding by the European Commission

The ruling means that Safe Harbor is no longer a legal basis for the transfer of personal data from the EU to the US, although technically it is for each member state to make their own decision on the basis of this judgement.

Privacy Shield

At the end of January 2016, the Commission announced that it had agreed (in principle) with the US authorities a new data protection framework to replace the now defunct Safe Harbor agreement. This new framework has been named Privacy Shield and will provide:

- Strong obligations on companies handling Europeans' personal data and robust enforcement. The Department of Commerce will monitor that companies publish their commitments under Privacy Shield, which makes them enforceable under US law by the US. Federal Trade Commission.
- Clear safeguards and transparency obligations on U.S. government access. For the first time, the US administration has given the EU written assurances that the access of public authorities to EU personal data for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used to provide access only to the extent necessary and proportionate to the purpose at hand.
- Effective protection of EU citizens' rights with several redress possibilities. Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. European data protection authorities will be able to refer complaints regarding mishandling of European personal data to the Department of Commerce and the Federal Trade Commission. A new Ombudsperson will be created to manage complaints regarding possible access by national intelligence authorities to EU personal data.

As of February 2016, the detailed text for Privacy Shield has not yet been drafted and so is still subject to review by the Article 29 Working Party. Review by the Article 29 Working Party, alongside critical scrutiny from privacy campaigners, may yet prevent the enactment of Privacy Shield. Even should Privacy Shield be enacted, the adequacy of the protection it provides is still likely to be challenged at the European Court of Justice. Organisations should keep a watching brief on the on-going development of Privacy Shield and consider alternative mechanisms to enable the legal transfer of personal data outside of the European Economic Area.

General Data Protection Regulation

The European General Data Protection Regulation (GDPR) completed the trialogue process (agreement between negotiators representing the European Council, Commission and Parliament) at the end of 2015. The Regulation is likely to be passed during 2016, however there is a grace period of 24 months prior to enforcement in order to allow affected organisations to adjust to their new obligations. The GDPR aims to harmonise European data protection law and make Europe as a whole a much safer place to store and process data. It places more emphasis on individual rights and increases transparency with respect to how personal data is used. It also increases the penalties for breaching the regulation to up to 4% of an organisation's global turnover. Other changes contained within the agreed regulation include mandatory requirements to conduct Privacy Impact Assessments, mandatory security breach notification and the need to obtain explicit consent from data subjects with respect to collection and usage of their personal data, including new controls on the use of profiling approaches. The GDPR also places increased emphasis on supplier due diligence by controllers such that they should only use those processors "…providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing". This will require cloud providers to be more forthcoming in terms of the security assurances offered so as to enable data controllers to make use of their services.

Organisations should not be overly re-assured by the 24 months grace period and should begin consideration of the implications of the regulation on their businesses sooner rather than later.

Data Sovereignty

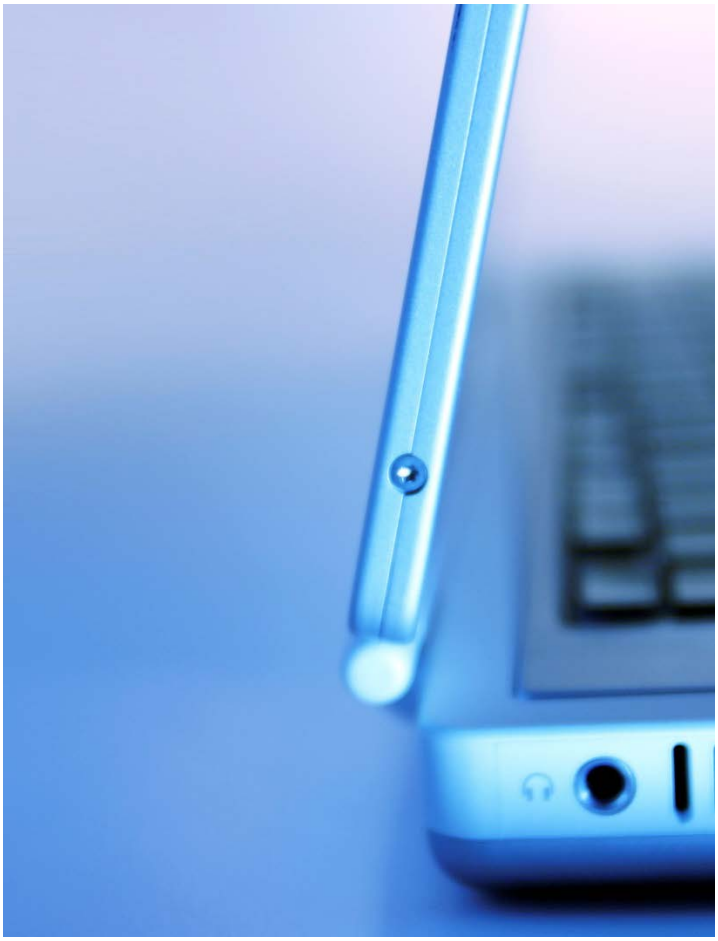
Increasing mistrust between jurisdictions about data, and the impact of other jurisdictions on the data, has led to a small, but growing movement for data localisation: the imposition of severe, legal restrictions on where data may be stored and processed. Russia implemented a law requiring Russian citizen data to be stored only in Russia in September 2015. Germany recently passed a law requiring communications data to be stored in Germany only.

Calls for a "European Cloud" – a cloud computing infrastructure determined by geographical borders – where example data created, processed, shared, accessed and managed must be stored and managed only within the borders of the European Union, are growing, and sharpened by the recent ruling on Safe Harbor. However, the value of such a proposition is questionable unless the entire supply chain is located within the trusted geography.

Although the derogations from the eighth principle of the DPA are a valid mechanism for export personal data from the EU, the EU model clauses and Binding Corporate Rules are still vulnerable to the issues that led to the invalidation of Safe Harbor, namely foreign surveillance, and foreign cloud provider's legal obligations under their home jurisdictions. Given the privacy lobby's recent success in overturning the Safe Harbor agreement, it remains to be seen whether they intend to subject these derogations to legal test too.

Global cloud providers are investing heavily in European data centres in order to avoid the complex and difficult issues associated with moving personal data out of the EEA. Even this last line of defence could crumble. Microsoft are currently fighting a case where the US has required them to hand over emails to the US federal government from its Dublin data centre. Many other US cloud providers have filed "friend of the court" briefs in support of Microsoft's defence.

If Microsoft loses its case, the US will have a legal precedent to the effect that US law prevailed over EU law in Europe for US service providers. This will have far reaching and profound ramifications on the role of the US service provider in Europe. A conclusion is not expected for many months, and therefore casts more uncertainty on the stability of the legal framework for transatlantic data flows. Even if Microsoft prevail, data owners should be aware that Mutual Legal Assistance Treaties exist that could still enable the US Government to access personal data held overseas, however the difference being that the access would be at the discretion of the host Government.



The Cloud is ready for consumers: Are consumers ready for Cloud?

Cloud providers have gone to considerable efforts to demonstrate that they have addressed the concerns of the market with respect to the security and data privacy of the information uploaded to their services. Some providers will also have robust and independently verified security credentials that are designed to meet the specific needs of the specific markets they are targeting.

However, potential consumers of cloud services also need to be aware of the changes that they should consider in order to make the most of the capabilities offered by cloud providers. Whilst it is often trivial to sign-up to use cloud services (on-demand self-service being one of NIST's essential characteristics), it is often not as trivial to push through the changes in culture, procurement, architecture and development/operations processes that drive home the benefits offered by the cloud approach.

Consumers should resist the temptation to apply old ways of working – technologically and procedurally – to cloud services. Organisations that have made the corporate decision to adopt cloud services should embark on a period of education to ensure that affected stakeholders are aware of the implications of the move to cloud. Some examples are discussed below:

— Procurement teams – the cloud enables rapid procurement of services and so substantial change for procurement teams that are more comfortable dealing with extensive OJEU procurement exercises. It is also critical to educate procurement teams on the differences between cloud providers and systems integrators so that incorrect assumptions on the services to be provided are not acted upon.

— Architecture team – it can be tempting to try and "lift and shift" old world legacy systems on to the new cloud-based environment. This is not usually conducive to recognising the benefits of the cloud model. Indeed, moving a complex system composed of interdependent services from a legacy data centre to the cloud can result in an increase in complexity, particularly if some elements of the system remain on-premises. Consumers should rather look to adopt cloud in a more managed and staged approach whereby legacy on-premises applications are retired and new applications, architected to make the most of the elasticity and automation offered by the cloud, implemented as part of the technology refresh cycle.

— Development and Operations teams – the adoption of cloud services is not happening in isolation of other developments within the IT world such as the adoption of Agile development approaches and the rapid, continual integration of changes to live services. The cloud model is ideal for supporting agile development but this may well impact upon the working practices (and traditional boundaries) between development and operations staff, especially if IT service management and improvement is not well established or integrated into the organisation or if the organisation chooses to go down the DevOps route.

— Security team – security has often been held up as a barrier towards cloud adoption. Security teams should be educated into the levels of control and automation that the cloud model offers; in many cases a cloud-based service will be more secure than the on-premises alternative. However, not all information will be suitable for hosting in all clouds; the security team should be able to offer advice on the categories of information that can be hosted on the public cloud versus the information that must be hosted on a private cloud or limited to on-premises.

— Staff – staff should be educated on the dangers of Shadow IT (i.e. the uncontrolled procurement of cloud-services by non-IT users) and advised to make use of central procurement routes to enable more controlled adoption of cloud services.

— Service management – whilst in many cases, particularly with PaaS and SaaS, there will be a shift away from traditional capacity management activities (such as monitoring of disk usage and CPU utilisation), this does not mean that service management is no longer required. Cloud services may charge per various thresholds, e.g. number of users, amount of data stored, number of transactions etc., and so service management will migrate towards a focus on threshold monitoring and management and away from the purely technical aspects.

Conclusion - the 10 key considerations for decision makers

This paper provides Senior Decision Makers with an overview of the security and privacy issues that should inform their decision-making when considering the implementation of cloud services. However, these issues are rapidly evolving as cloud providers continually improve their services and cultural awareness of cloud computing and cyber security rises. One area of particular uncertainty at the time of writing is that of privacy and data protection due to the on-going discussions relating to the implications of the Safe Harbor Agreement being ruled invalid, alongside the recent agreement on the contents of the EU General Data Protection Regulation. Those organisations considering the adoption of cloud services are therefore advised to consult with an independent source of expertise to validate their own understanding of the considerations described below prior to entrusting their data or services to a cloud provider.

In summary, the areas for consideration include:

— Organisational readiness: Ensure that relevant stakeholders within the organisation understand the implications of the cloud model for their functions and have plans in place to push through the relevant cultural, technical and procedural change.

— Develop a cohesive and consistent approach: Organisations will likely implement an ever increasing number of cloud services, across a variety of service and deployment models; organisations should have a clear and consistent approach to the management of cloud services, e.g. some of Service Integration and Application Management (SIAM) capability to enforce commonality and standardisation where possible.

— Evaluate the data and service: identify the types of data that may be required to be stored or processed in the cloud and note any regulatory or legislative requirements on the data or the service concerned.

— Determine the appropriate security wrap: identify the security controls that you need to be able to apply to protect the confidentiality, integrity and availability of the data and services to be hosted in the cloud; specify which of those controls are mandatory and which may be waived as part of an informed risk balance case. This security wrap must be informed by a comprehensive risk assessment of the services and data in scope.

— Evaluate the proposed cloud service: Map the required security controls on to the proposed cloud service(s) and identify where there are gaps in capability – or where the provider may offer services that allow an alternative approach to securing the data or service to be delivered. Document residual risk.

— Document responsibility splits: Identify where responsibility sits for delivery of the various capabilities (technology and process) – is it the provider or the data owner? It is a common mistake to find gaps in delivery responsibilities during implementation and it is usually far more cost-effective to document cohesive hand-over points between provider and consumer to fill any gaps in delivery responsibility as the cloud providers offer a standardised service.

— Evaluate the service provider: Conduct due diligence activities with respect to the service provider, e.g. financial stability, examination of independent assurance and accreditation statements, ethical and independence checks etc.

— Evaluate the service terms: Review the standard terms and conditions offered by the cloud provider and consider any additional clauses that may be available (e.g. some cloud providers offer additional enterprise data processing agreements) for relevance. Issues to consider include regulatory and legislative compliance, data location and jurisdiction, and exit, e.g. how long does the provider make data available for extraction after termination?

— Take the accountability test: Ensure that the justifications for the decisions taken with respect to the adoption of cloud services can pass the accountability test – is the decision justifiable to your customers, your Board, your shareholders or the Daily Mail if the worst comes to pass and the cloud service is compromised? Could the organisation bear the reputational damage if it was found to be storing sensitive data off-shore, or placing large contracts with providers that practised tax avoidance?

— Make an informed decision: based on all of the above, in particular a balancing of the residual risk and the expected benefits, make a defensible choice on whether or not to proceed with a cloud-based solution.

The Cloud First policy statement from Cabinet Office is strongly indicative of the preferred direction of travel within the public sector and also mimics a growing trend within the private sector. Very few organisations view owning, managing and operating data centres as a core business competency.

Cloud adoption is fast becoming the default option for new services, across many different sectors. After many years of being an up and coming trend, cloud computing is now established as a tried and tested delivery option; any organisation refusing to acknowledge the benefits on offer may soon find themselves being left behind by their users – and their competitors.

KPMG

KPMG

ANNEXES

Annex A – NIST definitions of Cloud Computing[17]

Key characteristics of Cloud

On-demand self-service. A data owner can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple data owners using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to data owner demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the data owner, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and data owner of the utilized service.

[17] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Cloud service models

Infrastructure as a Service – IaaS

The capability provided to the data owner is to provision processing, storage, networks, and other fundamental computing resources where the data owner is able to deploy and run arbitrary software, which can include operating systems and applications. The data owner does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service – PaaS

The capability provided to the data owner is to deploy onto the cloud infrastructure data owner-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The data owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service – SaaS

The capability provided to the data owner is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The data owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Cloud deployment models

Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of data owners from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid Cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Annex B - key contractual considerations

Data protection

Compliance with Data Protection Regulation is a fundamental requirement of all European cloud contracts, and must be reflected throughout the supply chain. Generally, the consumer of the service will be the data controller, and will therefore be liable for any breach of the act. There is currently no automatic presumption in the regulation that a data processer (generally the cloud provider) has any liability under the data protection act – unless the contract between data controller and data processor clearly sets out the respective liabilities. The Information Commissioner can levy heavy fines on an organisation found to be in breach of the data protection regulation, and these fines will become even heavier when data protection regulation is harmonised across Europe, expected to come in to law during Q2 2016 with a grace period of 24 months before enforcement

Compliance with other applicable legislation

Public sector buyers must ensure that their cloud providers and their sub-contractors comply with applicable legislation, including:

— Official Secrets Act

— Freedom of Information Act

— Prevention of fraud and bribery legislation

— Ant-terrorism legislation

— Equality and diversity legislation

— Tax compliance legislation

— Public Contract regulation

Public Contracts Regulations 2015

This came into force in February 2015. These regulations are designed to make procurement more agile and open, but also put obligations on providers in terms of their sub-contractors. This include the extension of mandatory grounds for exclusion to sub-contractors – which must be substituted if found to be in breach, and fair payment windows throughout the supply chain. A number of new mandatory grounds for exclusion have been included, including convictions for child labour, human trafficking, terrorist offences and binding legal decisions for non-payment of tax. It is now a discretionary ground for exclusion If an authority can demonstrate non-payment of tax or social security where no binding legal decision has been taken.

Law and Jurisdiction

Cloud computing often means that more than one legal jurisdiction will be involved in relation to any particular external cloud service. A cloud contract should specify which jurisdiction and laws govern the contract. Buyers will need to be satisfied that in the event of a dispute, that they would be comfortable enforcing contractual terms in an overseas jurisdiction, and that they understand the full legal implications of entering into a contract governed by overseas law.

Security

The DPA requires buyers to ensure that personal data is secure and protected from accidental loss, damage and destruction. Buyers must ensure that the cloud provider has adequate technical and legal measures in place to protect the data, and these measures must be proportionate to the nature of the data being processed and stored. Many cloud providers use externally validated accreditations and certifications to demonstrate their security credentials.

Audit rights

Buyers are accustomed to their contract with service providers containing clauses which grant the buyer a right to audit the provider. This is necessary to ensure the providers contractual and legislative compliance, but most importantly to ensure that the organisations information assets are being processed and stored in accordance with the terms of the contract. A buyer may want to invoke audit rights in the event of e.g. a security breach.

Many cloud providers find the granting of audit rights to a customer problematic, as the prospect of hundreds of customers invoking their rights would create an untenable overhead, and a security risk for other customers. Some cloud providers will compromise, by allowing a mutually agreed third party to conduct an audit, to then release the findings to any customer which requires it.

Sub-contracting

Buyers will need to understand whether any third parties will have access to their data, and for this reason, the extent and nature of the supply chain will need to be understood. This is particularly the case for SaaS services, who may use a third party infrastructure for hosting, including potentially other cloud services. In addition, buyers will need to be satisfied a cloud provider's liability for sub-contractor failure is included, rather than excluded, from the contract and that the sub-contractors are also complaint with regulatory, legislative and security requirements. The Public Contracts Regulation 2015 also puts certain obligations on the cloud provider, as prime contractor, to flow-down to their own sub-contractor(s), such as payment terms.

Rights and responsibilities

A good contract will clearly and unambiguously state the rights and responsibilities of both parties. Cloud contracts should not be any different in this respect. Buyers should have a thorough understanding of the respective responsibilities of both parties, and how risk is being apportioned, to enable informed decision making.

Intellectual property rights

Processing data in the cloud means that data is being added, modified, removed or generated. A cloud providers terms must clearly state where data ownership lies, including any new data.

Some cloud providers include terms that grant them a licence to republish some or all of the customer's data for the purpose of provision of the service. Buyers will need to satisfy themselves that the extent of any licence enables the buying organisation to remain compliant with the DPA, and to its third party obligations.

Limitations of liability and exclusions

Some cloud providers will put excessive limitations on their liability for service failures, data damage and loss, direct and indirect damages. Recent research by Queen Mary University London School of Law found that US cloud providers tended to seek to deny liability for direct damages as far as possible while European cloud providers were less overt about seeking to exclude direct liability, presumably because in most European legal systems it is difficult to do so. Buyers will need to be confident that they will receive adequate and proportionate compensation from the cloud provider, should anything go wrong.

Warranties

Research into cloud providers' standard terms by the Queen Mary University London School of Law showed that the cloud providers surveyed went to great lengths to deny that any warranty existed in respect of performance of the services, with US providers being particularly comprehensive with respect to excluding warranties. Buyers should therefore check this aspect of a cloud providers contract very carefully, and be prepared to try and negotiate a warranty if the contract terms are deficient.

Service levels and service credits

The vast majority of cloud providers will offer some form of service level agreement, although it is unlikely to be as comprehensive as those that a public sector buyer might expect under a typical IT outsourcing contract. The service levels will invariably be standard and non-negotiable. The onus is on the buyer to select a service level regime which meets the needs of the organisation, and which offers adequate compensation when service levels are not met.

Exit

Many cloud providers will not penalise a customer for leaving their service, and where a service is constructed and sold on a utility

basis, consumers can literally cease consumption of the service. As with any contract, buyers will need to check the cloud provider's terms to determine whether there are penalties for cessation of consumption or contract termination. Specific to cloud it the need to ensure that the customer's data can be retrieved, or is made available by the cloud provider, in a useable format that can easily be transitioned to a new cloud provider. Data owners should also be comfortable with the mechanisms used by their providers to render their data inaccessible upon exit.

KPMG

The contacts at KPMG in connection with this report are:

Lee Newcombe
Cyber Security
Senior Manager, Leeds, KPMG LLP

T +44 (0)11 3231 3629
M +44 (0)7468 711 307
E lee.newcombe@kpmg.com

Del Heppenstall
Cyber Security
Director, Birmingham, KPMG LLP

T +44 (0)12 1232 3080
M +44 (0)7467 339 438
E del.heppenstall@kpmg.com

Neil Clarke
Cyber Security
Senior Manager, Bristol, KPMG LLP

T +44 (0)11 7905 4183
M +44 (0)7825 504 524
E neil.clarke@kpmg.co.uk

www.kpmg.com

Produced by Create Graphics | CRT054154 | February 2016