



# Cloud UK

Paper six

A Buyers Guide to Cloud Services

6



## Introduction

**Cloud Computing is set to revolutionise the manner in which IT services are both delivered and consumed. Spurred on by the benefits of both operational flexibility and commercial efficiency, Cloud has become clearly established as a viable option for deploying IT services from organisations of all sizes and speciality.**

In the UK today over 50 per cent of organisations have formally utilised at least one Cloud service and satisfaction levels relating to that experience grew to an astonishing 96 per cent by the end of 2011. Furthermore, 85 per cent of IT Executives stated that they now formally considered Cloud as a viable option for delivering new IT projects within their wider IT strategy, signaling that the technical model has established a mainstream status among the profession.

In terms of future adoption, three out of four of those who have already purchased a Cloud service believe they will purchase further services for their organisation within 2012. Of those that have yet to adopt their first Cloud service, 18 per cent expect to do so in 2012, and a further 17 per cent intend to within three years. In fact only 4 per cent of the research base had no intention to ever use a Cloud service.

So the market for Cloud Services is set to grow more rapidly and this expectation is fuelling the growth in Cloud Service Providers (CSPs) and in diversity of the supply chain. Trusted suppliers are often changing their business models to embrace Cloud Services within their portfolio; 66 per cent of end users have expressed an increasing expectation of self service in light of the new service models enabled by Cloud Computing; and, a new breed of Cloud brokerages and aggregators are forming to provide commercial guidance and a single point of contact to customers.

What is important against this backdrop in any sourcing decision is to determine how a specific Cloud purchase or project will fall within the wider IT strategy of that organisation. The market has some way to go in terms of technical inter-operability and as such user organisations need to be clear on their data models and requirements for integration in order to be able to select and sew Cloud Services seamlessly into their IT operations.

Understanding what is possible with Cloud solutions and which deployment and service models exist is the subject of White Paper 5 (WP5). This Paper assumes familiarity with WP5 and is intended to provide guidance on how to approach a 'needs analysis' and how to shortlist and sift prospective Cloud Service Providers in order to determine both a best fit and reduce risk in meeting an IT sourcing goal.

The Cloud Industry Forum has established a Certified Code of Practice for Cloud Service Providers that aims to enhance standards by enabling end users to make a rational and informed choice in selecting a service provider by requiring information to be made available on essential matters and in a standard format. Whilst the CSP's certified against the CoP help end user confidence in selection, should you ever seek to assess a non CIF Certified company this White Paper will help to establish the key Information that you should request and review before making your selection.

85 per cent of IT Executives stated that they now formally considered Cloud as a viable option for delivering new IT projects



## Step one:

### Be clear on your needs and constraints:

Whilst it sounds like it is stating the obvious, many first time users of Cloud Services face scenarios that they have never had to face before because everything they did was constrained to their internal IT capability and as such issues were handled as they arose. The devil is in the detail and as there is no universal cloud proposition it is essential that thought is given to what is and isn't acceptable for the delivery of a Cloud solution. Making sure you are clear about what you are contracting for is the essential first step of any relationship with a Service Provider and therefore having a Requirements Document that details your specific needs will speed up and standardise answers from vendors if issued in the form of a Request for Information or Invitation to Tender.

As Cloud is all about distributed IT services it is a capability that has great potential to impact upon your wider business model. There are three areas of preparation which should be considered a guideline for groundwork in planning for Cloud adoption and which should be clearly thought through before you embark upon a selection process:

#### 1.1 What is the scope of the solution you seek?

- a. What are the essential features you need from a solution? Do you have a requirements document that sets these out for an RFI to score potential suppliers?
- b. In which geographies will you need to access and support the solution? Does the supplier offer commercial and operational support in these regions on local time zones and in local language?
- c. What is your minimum and/or maximum term of a contract you are seeking to enter?
- d. At what scale are you expecting to operate the solution (users or storage/processors etc)?
- e. How variable will that scale be? How much flexibility do you require in reducing capacity and at what intervals? Can you find a commercial model that is optimised to this requirement?
- f. How much of the solution do you want to be delivered to you as a service and which elements do you require to remain in control of? This will be a core influencer on the nature of the Service model that will be most appropriate.

Making sure you are clear about what you are contracting for is the essential first step of any relationship with a Service Provider

## 1.2 What is the rationale behind the need for the new solution?

Depending upon your internal justification for a new Cloud solution the issues that you will need to resolve will vary accordingly:

- a. New application/service:** Where cloud is being considered for new application areas not currently operating within your organisation, key drivers tend to be around lack of internal skill set, pressure on resource vs time-to-market needs, lowering financial risk etc. In such a scenario you need to consider what level of service is required from your service provider to ensure you can achieve your objective. If you do not want to be concerned with set up and configuration a more SaaS style solution will meet your needs, whereas, if you have very specific needs, an IaaS solution or Private Cloud may be more appropriate.
- b. Cost containment:** In main stream cloud adoption (i.e. after first experiences) cost reduction and containment tend to be the major driver for selecting this supply model. However, determining how costs are mitigated has a lot to do with the Deployment and Service Models you consider. By nature of their shared resources and generic capabilities, Public Cloud solutions and SaaS typically offer the lowest cost. However, even in large complex projects utilising Private Cloud (Deployment Model) or IaaS (Service Model), costs savings will arise through the consumption based pricing, mitigation of hardware and set up costs etc. Understanding your current cost base and setting a target for improvement will also be critical to ensure you can filter options meaningfully.
- c. Temporary Project:** If your need is for a specific time banded initiative (such as a proof of concept, research project etc) or is used periodically (stop/start such as seasonal business, system testing and QA etc) then cloud offers a viable and scalable solution. In this scenario focusing on issues around the contract term, ability to scale and shrink, data load and migration are going to be more relevant to your decision making.

Organisations will not move their business wholly away from an on-premise capability, especially where they have legacy IT solutions to manage

## 1.3 Do you have any fundamental constraints that need to be understood and complied with?

There may be influencers on your cloud solution that are not related to technology per se but rather relate to the environment within which your organisation currently operates. For example:

- a. Regulation:** Is your organisation required to comply with industry or functional regulation such as in the storage location and duration for data? (e.g. accounting, legal, healthcare). If so then understanding data location and protection will be a critical constraint, especially if the issue requires guarantees over geographic restriction of data. Such a constraint favours IaaS and Private Cloud.
- b. Legacy:** Does the solution you seek to implement have any interaction with, or replace, any legacy systems and infrastructure? Depending upon the answer, then specific Deployment and Service models may not be workable if networking is required. If the solution is being moved from on-premise to the Cloud, then there may be restrictions around issues such as O/S support or data load that favour one model over another.
- c. Integration:** Does the new solution need to be integrated with existing systems (e.g. a service management system that needs access to a CRM or Billing system to share customer data and workflow). If so this needs to be called out early on to determine if any SaaS solutions under review enable close integration.
- d. Connectivity:** What bandwidth constraints exist for your business and does this have any implication to the nature of the application being sought?

## Step two:

### Scoping those CSP's who are in the ball park:

**Buying online, whilst efficient, convenient and straightforward nevertheless by nature has a sense of the intangible about it. Traditionally IT has been delivered in an on-premise model where products are delivered to the organisation or its partner and are assembled, provisioned and managed. In the world of Cloud Computing that sense of reality is removed and rarely does anyone physically see the facilities within which their IT operations are housed. Whether buying direct online or via a third party it is essential that an organisation can establish confidence in the Service Provider/s so that they can be ultimately confident in both their expectations; in the nature of service provided; the responsibilities of the parties, and, the important issues to consider in entering, managing and ultimately exiting a contract.**

To assess the market and determine a short list of potential CSP's we recommend that you access the following information which should ideally be freely available for you to find on the target list of CSP's own websites:

#### 2.1. First things first, a proper introduction:

You cannot begin to have confidence in a service provider until you know who they are. Whilst a website may look polished, its pricing keen and its claims positive, how can you know if any of its content is true? The problem with a url is it is not a legal entity, but rather a reflection of a domain name that the legal entity has registered and through which its services are offered. So what is the physical presence behind the url and how do you reach the people involved in that business?

To establish identity and confidence in a vendor a number of facts are needed to build a full picture of the legal entity and structure of the CSP wishing to provide services to your organisation:

- What is the CSP's registered Corporate name and associated trading names?
- What is its legal status, date of formation, location of registration, and registration number?
- What is its ownership (major shareholders)?
- Who are the members of board of directors (or equivalent body)?
- Who are the Executive management responsible for running the company?
- Where is its corporate fixed address (not a PO Box)?

Be very wary of organisations that do not declare their physical address and contact numbers, preferring to push for you to do everything online. Convenience is one thing, and a choice you can still exercise, but you need to know the substance of who you are dealing with and have knowledge of how to reach them if your online experience is not sufficient.

Whether buying direct online or via a third party it is essential that an organisation can establish confidence in the Service Provider/s

## 2.2 What service/s can the CSP provide?

An online process should, by nature, be structured to present information in a manner that drives efficiency in selection. However, mapping your organisational needs in a relevant format can be a challenge and being able to compare solutions between vendors requires a common set of data to be available.

A presales capability on the website, or downloadable PDF's, will typically answer basic questions about the feature set of the services offered and should enable a rudimentary mapping of needs to capabilities. However, gaining clarity on where the CSP has commercial (sales and support) and operational (data centres) presence will help to determine how that organisation is placed to support your needs. For example:

- Have they a presence in your operational territory/ies?
- Are they accessible 24/7? How – email? Voice?
- Do they operate their own data centres or rely on third party facilities?
- If they operate in multiple international territories can you as a customer dictate in which territory/ies you want to restrict your data to be stored and processed in order to meet any regulatory or compliance needs?
- Does the CSP offer levels of backup and restore for the services they provide?
- Do they offer data migration services to aid on-boarding at contract start and migration at the end of the contract?

Each of the above questions have little or no bearing on the actual features being delivered but are critical to understand the limits of what is and isn't being offered in terms of the wider service scope.

## 2.3 Supply chain length and liability

Clarity will be needed to understand how the service is delivered to you and who is accountable and liable for service delivery:

- Is the party selling the service to you actually providing the service or reselling the service?
- Does the CSP operate its own data centres or rely on a third party?
- Are all elements of the service under the direct management of the CSP or are third parties involved?
- To what extent does the CSP accept indirect responsibility for their suppliers (if relevant). This is important to understand if any party in the CSP's supply chain went out of business, such as collocation where services could be taken off-line.
- To what extent do the CSP's suppliers (if relevant) accept indirect responsibility to the CSP's customers? E.g. if the CSP went out of business, can the end user work with the upstream providers to ensure continuity of service? If the CSP aggregates third-party services that are on-sold to the CSP's customers, do the third-party supplier contracts offer reciprocal terms and protections e.g. liability, service level resolution, data protection?

Clarity will be needed to understand how the service is delivered to you and who is accountable and liable for service delivery

#### **2.4 Security principles**

What mechanisms does the CSP operate in regard to access control, data storage and data in transit to ensure compliance with data protection as well as offer effective security and sovereignty?

#### **2.5 Understanding the benefits and pitfalls of technology**

Does the CSP utilise any specific technology platform/s (e.g. hypervisor, O/S, Storage threshold) and are they compatible with the solution sought or provide any restrictions that need to be understood? Equally do they offer any unique technology that may be attractive in terms of feature set or efficiency or management?

Conversely, does the choice of technology and process provide any barriers to changing CSP's in the future? Are you able to migrate your data in a practical time-frame at the end of an agreement (however reached)? Are there any lock-in or inter-operability issues to mitigate?

#### **2.6 Independent professional recognition:**

Does the CSP achieve and maintain any relevant certifications which show a commitment to accountability and professional conduct, e.g. CIF Code of Practice, ISO 9001, ISO/IEC 27001, PCI DSS, SAS 70/SSAE 16/ISAE 3402? Is the scope of their certification relevant to the services you seek?

## Step three:

### Applying the fine filter on your short list:

Assuming that the probing outlined in Section 2 highlights a number of potential organisations that may meet your operational needs, it is important to get to greater detail with your shortlisted candidates as you will be relying on them for operational delivery of elements of your IT for some time. The following outlines the detail that the Cloud Industry Forum requires any CSP's who wish to be Certified to make available in the contracting process to ensure an end user has sufficient accurate detail upon which to base a buying decision. (Depending on your commercial process a CSP may stipulate the information is confidential and may require a simple Non Disclosure Agreement to be entered into to protect their commercially sensitive data which is fair and reasonable).

#### 3.1 What are the commercial terms of supply?

- Pricing policy (basis of charging with fully-declared costs to enable predictable costs to be determined).
- Payment terms (what are mechanisms for payment, days of credit and penalties if any).
- What contract length options exist and is there discount for longer commitment?
- What are the options for termination by either party, and the associated conditions?
- What is the process for contract renewal and amendment terms and process?

#### 3.2 What is the personnel profile of the CSP?

- How many people are employed in the CSP's business to deliver the service you are seeking? How many are based in the regions/you are looking to operate in?
- Does the CSP operate effective employee vetting procedures and do they restrict access by their employees to your data?

#### 3.3 What are the customer migration paths at contract termination

Require a declaration from the CSP of any commercial restrictions in their solution:

- Technological implications (e.g. is there technological lock-in that prevents migration to other suppliers or in-house).
- Format of data provision and transfer (and timescale) at the end of the agreement.
- Cost implications (e.g. are there any costs associated with recovering data, or for purchasing replacement licenses?).

#### 3.4 What are the customer migration paths during contract execution

- What implications are there in the event of the CSP itself, or their suppliers, changing their provision of services, or ceasing business (e.g. is there technological lock-in with a specific supplier in the chain?).
- What is your commercial and technical options/ability to retrieve data in such situations?

### 3.5 Who is accountable for software licensing?

- Clarify who is responsible for any software/IP licensing of the solution, and any costs involved which are not covered within the cost of the services being provided. For SaaS this is more likely to be the CSP's responsibility, but for IaaS and PaaS this is more likely to rest with the customer unless otherwise stated.
- Are there any licensing implications in addition to cost, including in particular whether \*GPL code is used (potentially requiring publication of all code whether original code modified or not).

### 3.6 What provisions are made for information security

- Overview of measures in place to provide for information security in general.

### 3.7 What data protection provisions relate and how are they covered?

- In which countries and locations your data will/may be held during the term of the contract, and where processing will/may take place including for backup purposes.
- Which Data protection legislation will be relevant to the contract?
- Overview of the measures taken to ensure compliance with relevant legislation and to ensure data privacy?

### 3.8 What provisions are made for service continuity?

- Request an overview of the CSP's measures, including redundancy of operations, to provide for service continuity including protection against data loss.
- Is there a chargeable option for bespoke backup and recovery solutions?

### 3.9 Do you have any right of audit?

- From an attitudinal and transparency perspective, what ability will you have to arrange independent audits of the CSP's organisation for various purposes, e.g. security, license compliance and CIF audits ahead of during the term of an agreement?

### 3.10 Are there any service dependencies in the supply chain?

- Request a documented outline of the service elements and any dependency on third parties the CSP has to deliver your service (including any sub-contracting or co-location relationships (names may or may not be given).
- What are the implications of service dependencies for achieving service levels and compliance with data protection requirements?

### 3.11 What are the complaints and escalation procedures in operation?

- What is the mechanism and SLA for raising and resolving complaints?
- What is the escalation procedure and are their named individuals for escalation?

Once the above data has been collated and cross checked between potential CSP's and compared to the needs analysis you have created you should be able to score those more likely to meet your service requirements and have clarity on the issues you need to manage either in contracting or in your own organisation to compensate for any shortcomings you may have identified. Following this a final stage of validating the operating practices of your preferred supplier should be carried out (as per Step four) to understand the practices they operate and to determine the way in which you will need to manage service delivery to meet your expectations.

you should be able to score those more likely to meet your service requirements and have clarity on the issues you need to manage

## Step four:

### Understanding capability and practice:

**As you are entering a form of partnership with a CSP' it is essential that you have the ability to understand their operating practices and procedures in order to ensure you exercise appropriate controls and monitoring and therefore align your own practices to reduce risk and improve service availability and performance.**

All credible CSP's should have a documented management system that covers their operating practices and policies and should include, at a minimum, (a) written policies and procedures, (b) specific individuals assigned with relevant responsibilities, and (c) appropriate training and awareness programs. These requirements are similar to, but less onerous than, full management system standards like ISO 9001 (quality management), ISO/IEC 27001 (security management), and ISO/IEC 20000-1 (service management).

The specific areas for which documented management systems which we would encourage you to be aware of in signing up with a CSP are as follows:

1. Information Security Management (including Data Protection).
2. Service Continuity Management.
3. Service Level Management.
4. Supplier Management.
5. Software License Management (including License Compliance).
6. Complaint Handling.
7. Environmental Impact Management.

The first four of these are areas specifically covered by ITIL® V3, for reference by organisations seeking general guidance. The last three are not explicitly covered in ITIL V3 at the same level, but are considered critical to success for organisations operating in the Cloud Industry.

The extent of documented systems exist are likely to vary depending on the CSP's size. For a large multi-national CSP, there will likely be extensive policy and procedure documentation. For a small two-person CSP, the documentation requirements will be limited, but a minimum level of documentation will still be needed.

It should be possible to access customer facing versions of these procedures and policies under a commercial Non Disclosure Agreement and we recommend that this is requested before signing a definitive agreement.

All credible CSP's should have a documented management system that covers their operating practices and policies

## Appendix:

### The short cut:

#### Look for the Cloud Service Provider Code of Practice:

The purpose of CIF's Code of Practice for Cloud Service Providers ("Code") is to bring greater transparency and trust to doing business in the cloud, and it is the customer experience which is ultimately the most important for achieving this.

The customer experience operates on several levels:

#### Trust

Knowing that an organisation meets the requirements of the Code gives prospective customers assurance that it can obtain the essential information necessary to make competent sourcing decisions. The Code of Practice Certification Mark by itself conveys this assurance.

The Certified Mark identifies an organisation that has Self Certified to the Cloud Service Provider Code of Practice and the public declarations are accessible both on the suppliers website and the CIF website Register of Certified Organisation.



#### Identification of suppliers

The Code scheme helps customers identify suppliers at three different levels:

1. The fact that an organisation is listed on the CIF website as certified will enable prospective users to access those organisations (via hyperlinks) which have demonstrated this level of responsibility.
2. Organisations which have registered to begin the process of Self Certification can opt to have this status shown on the CIF website, and customers may select from them as well.
3. A freely available on-line searchable database of services offered by certified organisations is accessed via the Cloud Industry Forum Website.

#### Access to information:

A customer is always able to obtain the publicly-available information (covered by the Code) from the certified organisation's web site.

A customer is also able to obtain a copy of the publicly-available information submitted with the Application from CIF's website.

#### Monitoring of the Code:

CSP's claiming compliance with the Code shall conduct an annual Self-Certification and confirm the successful results of this Certification to the CIF in order to receive authorisation to use the Certification Mark (the 'logo') for the following year.

The CIF will spot check and randomly audit Self-Certifications as well as investigate any formal complaint of non-compliance against an organisation claiming compliance with the Code. In the event of finding a false declaration or material non-conformity, at the sole discretion of the CIF, the authorisation to use the Certification Mark shall be immediately suspended, pending resolution, or terminated, and this action shall be documented on the CIF website, and may be reported publicly such as via press releases.

#### Further reading

- |                       |   |
|-----------------------|---|
| CIF White Paper three | Negotiating Cloud Contracts             |
| CIF White Paper five  | Cloud definitions and Deployment models |

Knowing that an organisation meets the requirements of the Code gives prospective customers assurance that it can obtain the essential information necessary to make competent sourcing decisions



**The Cloud Industry Forum (CIF)** was established in direct response to the evolving supply models for the delivery of software and IT services. Our aim is to provide much needed clarity for end users when assessing and selecting Cloud Service Providers based upon the clear, consistent and relevant provision of key information about the organisation/s, their capabilities and operational commitments.

We achieve this through a process of self-certification of vendors to a Cloud Service Provider Code of Practice requiring executive commitment and operational actions to ensure the provision of critical information through the contracting process. This Code of Practice, and the use of the related Certification Mark on participant's websites, is intended to provide comfort and promote trust to businesses and individuals wishing to leverage the commercial, financial and agile operations capabilities that the Cloud based and hosted solutions can cover.



**The Cloud Industry Forum**

Sword House, Totteridge Road  
High Wycombe HP13 6DG

t 0844 583 2521

e info@cloudindustryforum.org

www.cloudindustryforum.org

