

Practice Guide for Procuring Cloud Services



Published by
the Office of the Government Chief Information Officer
(November 2013)

Disclaimer

The information provided in this Practice Guide for Procuring Cloud Services (“the Guide”) is for general reference only. It does not provide an exhaustive guide on procuring cloud services. The Government of the Hong Kong Special Administrative Region (“the Government”) makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information provided in this Guide.


This Guide also contains information input by other parties and readers may link from this Guide to other sites and obtain information provided by other parties (collectively called “the other information”). The Government expressly states that it has not approved nor endorsed the other information contained in or in connection with these sites.

The Government does not accept any responsibilities for any loss or damage whatsoever arising from any cause whatsoever in connection with this Guide. The Government is entitled to add, delete or change any information in this Guide at any time at its absolute discretion without giving any reason. Readers are responsible for making their own assessments of all information contained in or in connection with this Guide.

Practice Guide for Procuring Cloud Services

Table of Contents

Introduction	3
Basics of Cloud Computing	3
This Practice Guide.....	4
Cloud Computing Service Models.....	4
Deployment Models.....	6
Key Area 1: Service Cost.....	9
Current Market Situation	9
Key Points to Note.....	9
Key Area 2: Service Level	12
Service Level Agreements (SLAs)	12
Service Level Objectives (SLOs).....	12
Key Area 3: On Boarding & Off Boarding	16
Overview	16
Data Migration	16
Service Billing and Metering	17
Data Retention	17
Key Area 4: Service Operation	19
Service Operation.....	19
Best Practices	19
Service Desk	20
Build up Service Governance Strategies	22
Key Area 5: Security and Privacy Protections	24
Key Area 6: Service Commitments / Warranties	26
Current Market Practice.....	26
Standard Terms of Service	26
Pre-contractual Statements	27
Matching the User's Requirements	27
Reading the Fine Print - Disclaimers	28
Are the Commitments Appropriate?	29
Key Area 7: Data Ownership & Location and IP Ownership	30
Current Market Situation	30
Key Points to Note.....	30
Key Area 8: Service Default.....	32



Current Market Practice.....	32
Overview	32
Frequent Limited Reciprocal Obligations.....	33
Excused Non-Performance.....	34
Remedies.....	34
Termination	35
Damages and Limitation of Liability.....	35
Specific performance	36
Conclusion.....	37
Key Area 9: Contracting (Terms of Service).....	38
Current Market Situation	38
Role of the Contract	38
Contracting for Cloud Computing	39
Be mindful of the source.....	40
Steps for Contracting for Cloud Computing Services.....	42
Conclusion.....	45
References.....	46

Introduction

Basics of Cloud Computing

In simple language, cloud computing is the delivery of computing resources (hardware and software) by a party (the service provider) over the Internet to a user¹. This delivery or provision is described as a “service” because the user merely uses the computing resources rather than actually acquiring them. It provides shared computing resources to achieve economies of scale similar to a public utility (like the electricity grid).

With cloud computing, users can in effect “rent” computing resources (application software, hardware platforms, storage, etc.) without the need to acquire (and install) the respective hardware or software items. The cloud service provider manages the infrastructure and platforms on which the applications run, as well as security. All the user must do is access the computer resources via the Internet from the user’s device. It allows the cloud service user to get its applications up and running faster and to adjust resources more rapidly to meet fluctuating and unpredictable business demand.

Cloud computing offers many potential benefits to small and medium enterprise (SME) users, but may incur potential risks as well. Successful business has always been an exercise of balancing risk and reward — and cloud computing is no different. As a variation of IT outsourcing, it should not be surprising that many of the risks of cloud computing are the same or similar to the risks in more traditional IT outsourcing. And many of these risks can be mitigated the same way:

- appropriate due diligence up front;
- strong contractual protections that account for higher risk data and applications;

¹ In discussions about cloud computing, the “user” may be also be referred to as the “customer,” “consumer” or “buyer”. Such references may be used interchangeably in this Practice Guide.

- appropriate service level monitoring by the service provider and the user;
- consider the exit arrangements (ease, speed and cost); and
- build up service governance strategies.

This Practice Guide

This Practice Guide is intended for local companies, in particular SMEs, to assist them in building their understanding of cloud computing and how it may bring benefit to them, but also how to evaluate and consider some of the risks associated with incorporating cloud computing into their operations. In this regard, it requires the company considering a cloud computing solution, to exercise sound judgment in comprehensively evaluating its own requirements with respect to an available cloud computing solution and the extent to which that solution meets those requirements.

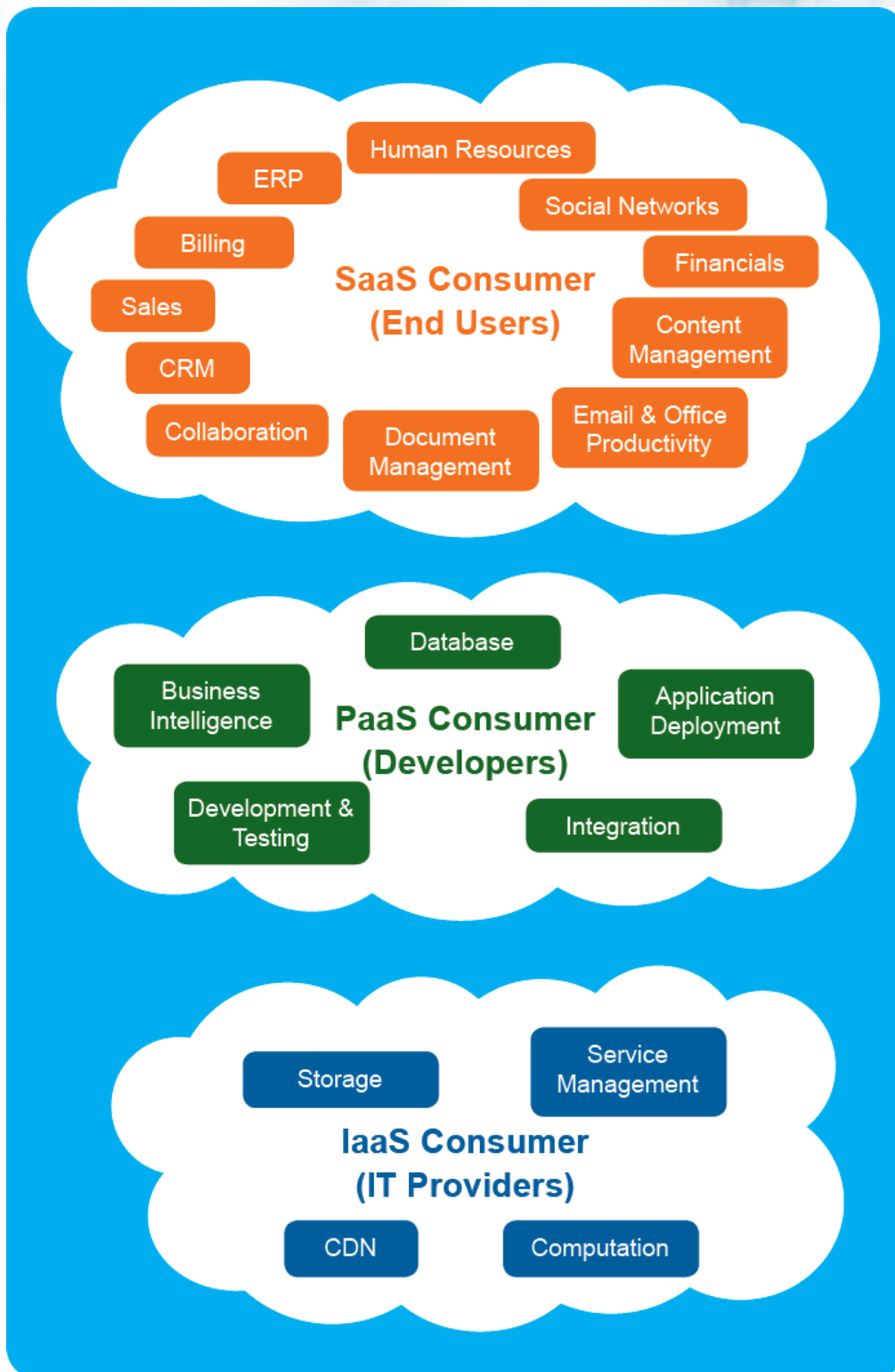
Cloud Computing Service Models

There are three kinds of cloud services, and these are referred to as “service models”:

- **Software as a Service (SaaS)** provides applications running on a cloud infrastructure that can be accessible by the users through various client devices. Examples of such applications include accounting, collaboration, customer relationship management (CRM), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management services, etc.
- **Platform as a Service (PaaS)** provides facilities for application design / development, testing, deployment and hosting as well as platform services for team collaboration, web service integration and marshalling, database integration and developer community

facilitation, etc.

- **Infrastructure as a Service (IaaS)** provides processing, storage, networks, and other fundamental computing resources where the users are able to deploy and run their own software. Examples of such services include storage, computation, content delivery network (CDN), service management, etc.



Deployment Models

There are 4 deployment models for cloud services.

- **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 organisation, or some combination of them. It exists on the premises of the cloud service provider.

- **Private Cloud** - The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple users (e.g. business units). It may be owned, managed, and operated by the organisation (an in-house Private Cloud), a third party (an outsourced Private Cloud), or some combination of them, and it may exist on or off premises.
- **Community Cloud** - The cloud infrastructure is provisioned for exclusive use by a specific community of users from organisations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **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 standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

A comparison table for the four deployment models is given below.

Aspects	Public Cloud	Private Cloud	Community Cloud	Hybrid Cloud
Provisioning Model	Provisioned for open use by general public	Provisioned for exclusive use by a single organisation	Shared use by a specific community of organisations	Combination of two or more distinct cloud infrastructures
Costing / mode of payment	Utility pricing (“pay-per-use”), no upfront capital costs	Capital investments required for initial setup	Cost contributed by individual organisations	Mix of private and public cloud pricing
Service Level Agreement (SLA)	SLA defined by service provider	SLA defined by the organisation	Shared SLA by participating organisations	Mix of different SLA’s
Possible Use	Handling open / non-sensitive data with large variations in demands	Mission critical systems / handling sensitive data	Community of organisations with shared business needs	Mixed business needs

Key Area 1: Service Cost

Current Market Situation

The charging schemes of public cloud services are often characterised by a pay-as-you-go model with minimal or no upfront costs. Computing resources are packaged in a form of services that is commoditised and delivered in a manner similar to utilities like water and electricity. Users can flexibly consume more or less resources as and when needed. Services charges will be based on demand.

Among the 3 types of cloud services, namely, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), IaaS are typically charged based on unit rates of allocated/used computing resources per unit of time. Charging schemes for PaaS and SaaS of different service providers vary and are application specific. Examples of charging schemes of PaaS and SaaS are based on number of users per unit of time and allocated disk storage per unit of time.

Computing resources in IaaS commonly include server, storage and network. The charging will be based on size of servers, typically expressed in terms of number of virtual CPUs (viz vCPUs), and size of allocated memory; size of disk storage and Internet bandwidth allocated/consumed. Some service providers charge these computing resources separately whilst some providers charge them together as bundled offers (in the form of a virtual machine, or VM).

Key Points to Note

Need to compare charging rates

- Charging rates are typically expressed as \$ per unit of virtual computing resources. However, the performance of a VM or vCPU would vary, quite significantly, depending on the physical

infrastructure of different service providers. Users need to look for more specific performance information (e.g. performance of a vCPU expressed in terms of performance of a CPU core) of the virtual computing resources for comparing objectively the unit rates among different cloud service providers.

- Factor in the software and services bundled when comparing unit rates. Apart from core computing resources (i.e. servers, storage, Internet bandwidth), service providers may bundle system software to subscribed virtual servers in their unit rates. IaaS providers usually bundle operating system software (typically Linux or Windows), and some providers also provide additional software (e.g. database, application software) either in a bundled manner or in separate unit rates. IaaS providers may also bundle support services (e.g. service desk and its support hours, anti-virus) with varying extents.

Need to study the details

- Understand the charging details, e.g. the units of measurement for charging, whether the resource is charged on allocation-based or usage-based, any upfront payment, any minimum charge, the billing cycle, any commitment of minimal usage, any volume discount, any extra charges imposed in respect of usage beyond specified quota or limit, and other extra charges not bundled in the unit rates (e.g. migration cost at service inception).
- Depending on the charging scheme, unused computing resources (such as an idle VM) may be charged or not. Users should ask the service provider for any mechanisms to allow them to disable or switch off unneeded computing resources to save cost.
- Find out whether there will be any rebate of service cost or service credit if the service provider fails to achieve the committed service levels.
- Ask for any arrangements to support users' ongoing monitoring on usage and charge of the services subscribed / consumed. This will avoid dispute when unexpected bills are received at the end

of the billing cycle.

- On a usage-based charging scheme, users may not easily estimate the actual usage of resources and thus the charges. Users should ask the service provider for timely alert when they detect an exceptionally high usage (e.g. due to user program bugs).
- Be aware of the unexpected cost. For example, a user may face software upgrade costs that were not expected when the user moved an existing application to a cloud platform.

Need to consider exit arrangement

- Understand if there is any minimum committed period of usage as well as any penalty for early contract termination.
- Find out whether there is additional cost of bringing out virtual servers, data, and software licence at contract termination.

Key Area 2: Service Level

Service Level Agreements (SLAs)

An SLA defines the interaction between a cloud service provider and its user. An SLA contains several things:

- A set of services the provider will deliver and a complete definition of each service.
- A set of metrics to determine whether the provider is delivering the service as promised and an auditing mechanism to monitor the service.
- The responsibilities of the provider and the user, and remedies available to both if the terms of the SLA are not met.
- A description of how the SLA will change over time before contract expiry under different circumstances.

There are two types of SLAs – off-the-shelf agreements and customised, negotiated agreements. To the extent public clouds service providers offer SLAs at all, most are off-the-shelf SLAs that are non-negotiable.

Service Level Objectives (SLOs)

An SLA contains service level objectives (SLOs) that define objectively measurable conditions for the service and set the expectation of service. Each service level objective has a metric, i.e. what to measure, and a target value.

In general, there are several points we need to consider in evaluating an off-the-shelf SLA or in reaching a service agreement with cloud service provider.

- Relevance of the defined service level objectives – whether the selected metric has a close relationship to the service attributes. For example, the metric for system uptime has a close relationship to the availability of service.
- Sufficiency of the defined service level objectives – whether the selected metrics are able to provide a full picture of the service. For example, if the metric for responsiveness is not in place, then the status of the service cannot be fully reflected. Say, the system could meet the uptime target, but its response time might be so slow that users cannot get their work done in an efficient manner. Examples of service level objectives for cloud services are: availability, response time, time for provision of computing resources, etc.
- An appropriate target value for the selected metric – Too low a target value may not be able to attain the business objective of subscribing cloud service. On the other hand, too high a target value may not be achievable.
- How to measure and monitor the defined service level objectively?
- What is the consequence if a service provider fails to meet the service level? Does the user have a business contingency plan?

Having said the above, usually, service providers already have sets of service level for their users.

As there are three types of cloud computing service models: IaaS, PaaS, and SaaS, they have different service levels and service operations.

The following table shows some of them.

Service Model	Service Provided	Service Level	Service Operation
IaaS	A mere computing environment (CPU, memory, network, storage) usually with the basic operating system	<ul style="list-style-type: none"> • Environment provisioning time • Environment availability • Environment performance 	Usually, users create, change and backup the computing environment through a service portal.
PaaS	<p>Environments for program development, testing and production run.</p> <p>It may include Web server, database server and application server.</p>	<ul style="list-style-type: none"> • Service levels stated for IaaS are applicable. • Under PaaS, it is a service provider to take care of the underlying infrastructure, such as patch update and version upgrade. Thus, service level may be used to govern a service provider to announce the infrastructure change ahead of time and provision a patched or upgraded environment for testing out application compatibility and performance. 	<p>Regarding infrastructure maintenance and update, the service operation should be transparent to users. However, when such operations affect availability, users should be well and duly informed of the schedule and impact.</p> <p>Since the application and business process are developed by users, they need to take care of the corresponding operations, such as backup of database containing business data.</p>

SaaS	Application	<ul style="list-style-type: none"> • Application availability, such as application uptime • Application performance, such as application response time • Under SaaS, from infrastructure to application all are taken care by a service provider. Users should be duly informed of the changes and be given the related environment for testing. 	Under SaaS, users interact with application only. The operations of a service provider are transparent to users, unless it affects availability and performance.
-------------	-------------	---	--

Though the service operation by a service provider should be transparent to users, there are two points worth noticing. They are data security compliance and incident management. Data security is about how service provider secures users' data. It is important users' data should not be leaked. Incident management is about the capability of restoring normal service operation as soon as possible when incidents causing service disruption happened.

Key Area 3: On Boarding & Off Boarding

Overview

Using cloud computing services will require some changes to current network and system infrastructure in order to gain the benefits of elasticity and cost-saving of cloud services.

On-boarding is the process and steps that the user needs to take when moving to cloud service, including moving data to cloud services provider platforms. As with any technology transformation, a user making changes involving moving data and data processing functions to a cloud solution will require lifecycle (project) planning and also risk mitigation steps. On the other hand, off boarding is the process of the user moving off a cloud solution, where the focus must be to ensure the user's data are securely retrieved and migrated (and, as appropriate, deleted from the service provider's platforms) when the user is either changing cloud services provider or stopping cloud services all together.

Users should work with cloud services providers in the on-boarding and off-boarding processes in order to ensure smooth transitions. The following areas shall be studied:

- Data Migration
- Service Billing and Metering
- Data Retention

Data Migration

- When the cloud service is a replacement of current infrastructure (such as email or human resources system etc.), the user will need to copy or move a large amount of company data to the chosen cloud platform. The user should review the options offered by cloud service provider on data migration and in particular on tools

or documentations. When the data migration involves complex systems and data conversions, the user should be aware of the additional costs.

- The data migration costs and time should be well defined, for example data transfer fee and support services fee. The user should prepare system and data inventories, at the same time, cloud services provider should list options and pricing.
- The user should ask and clearly understand how the cloud service provider addresses the issue of data leakage and protects data. For example, whether a user can have a safe path to migrate the data over SSL gateway and the ability to choose whether to store the data encrypted or not. The encryption methodologies should cause insignificant impact on performance (limited to between 10% - 15% performance reduction).

Service Billing and Metering

- As cloud services are billed regularly based on usages, the user should establish process that reviews and approves cloud services related billing and metering. This will ensure billing items and usages are directly matched.
- Some cloud services providers offer cost forecasting tools or usage notification services. The user should enrol such services if available.

Data Retention

- When terminating cloud services, the user has to decide on how the data stored in cloud platform should be handled. Options include deleting the data, migrating the data to another provider or archiving data at the original cloud service provider.

- Storing unused or outdated data on cloud platform even when it is not accessed may incur some costs. The user should also be aware that price on moving and accessing unused data may be different from ordinary pricing.
- Before terminating the contract, the user should ensure all data are deleted; this should include testing data and backup copy. When the data contain personal data and are regulated by Personal Data (Privacy) Ordinance (Cap 486) of Hong Kong, the user should ensure cloud service provider properly deletes all of the data.
- Cloud service providers' commercial activities, such as business liquidation, acquisition or merger, affect existing service and data retention. The user has to carefully read terms and conditions to check if the data stored with the existing service provider can still be obtainable or may be transferable under such business change.

Key Area 4: Service Operation

Service Operation

Simply speaking, the objectives of service operation are about how a service provider can deliver service to their users in a secure, reliable and high-quality way, including in a manner meeting any agreed SLAs. Ideally, the operation of a service provider should be transparent to users. However, the changes made by a service provider could bring impact to the service delivered to users. Besides, an incident (problem) management process has to be in place to handle incidents impacting users. Change control is necessary to assure the service to users. For example, in an IaaS context, for a change, such as an upgrade of operating system, etc, the service provider should duly inform users of the changes and provide an environment for the affected users to test out whether there are adverse impacts brought by the change.

Cloud computing represents a significant shift from the conventional norms of an organisational data centre to a de-perimeterised infrastructure open to use by potential adversaries. As with any emerging information technology area, cloud computing should be approached carefully with due consideration to the service operation of the service provider. The responsibilities of both the user and the cloud service provider vary depending on the service model selected. However, understanding the policies, procedures, and technical controls used by a cloud service provider is a prerequisite to assessing the quality of services and the security and privacy risks involved, and ultimately its viability for the user.

Best Practices

It is desirable to compare the service provider with the industry best practices of the service operation, e.g. security best practices to run their services operation.

Quality Management

- Quality manual
- User Satisfaction
- Continual Improvement
- Internal & External Audit
- Certification e.g. ISO9001

IT Services Management

- Service Desk
- Incident and Problem Reporting
- Change Management
- Configuration Management
- Certification e.g. ITIL, ISO/IEC 20000

Security Management

- Information Security Manual
- Business Continuity Planning (BCP)
- Continual Improvement
- Internal and External Audit
- Certification e.g. ISO 27001

Service Desk

A service desk provides a single point of contact for users to report any issues they may have with the service. It generally serves problem resolution, service restoration and system support. There are varying support levels in cloud service providers.

- Basic support might mean a few days response time via a Web-based portal where the question is asked.
- It might also simply mean access to a web-based discussion forum for experience sharing amongst the user community.
- A premium package may shorten the response time to a few hours, but no guarantees about service levels.

- Some providers state that they will provide a one-hour response time for “urgent” issues. Users must clarify what “urgent” actually means.

Communication Means and Call Logging

The service provider should support a wide variety of communication channels, including phone, email and online forms. User calls in all forms should be recorded to make follow-up easy and traceable.

Knowledgebase

If service desk personnel do not have the right information to do their jobs, their jobs cannot get done well. Knowledge management ensures that people get the information they need to do their jobs correctly. Service management systems often link to a database for past incidents and how they were resolved; this database speeds up incident resolution.

The scope of support service has to be evaluated before subscription. Some service desks can deal with issues beyond incident and problem reporting, such as change management, customisation, and so on.

Incident and Problem Reporting

The service desk should support the assessment, prioritisation, resolution, notification, and reporting of incidents and problem severity.

Users should ask the cloud providers how they deal with various circumstances or issues such as the following:

- Configuration management: Someone made an error while changing a configuration.
- Network: The network gets overloaded.
- Database: A database table needs to be optimised.
- System management: A processor of a server failed and the failover did not work.
- IT security: A denial-of-service attack is in progress.
- Application: A program has a bug.

Change Management

Suppose the users want to customise their applications or need some other type of support, the service desk should support the management of change requests, including information about how system components interact. Often, the provider will include some support for customisation in the contract. This might consist of one-on-one interactions with a staff from the cloud provider.

Configuration Management

The service desk should support mapping resources to the business processes that they support. Configuration management often entails a Configuration Management Database (CMDB) or some other kind of data store for holding all the cloud data centre assets.

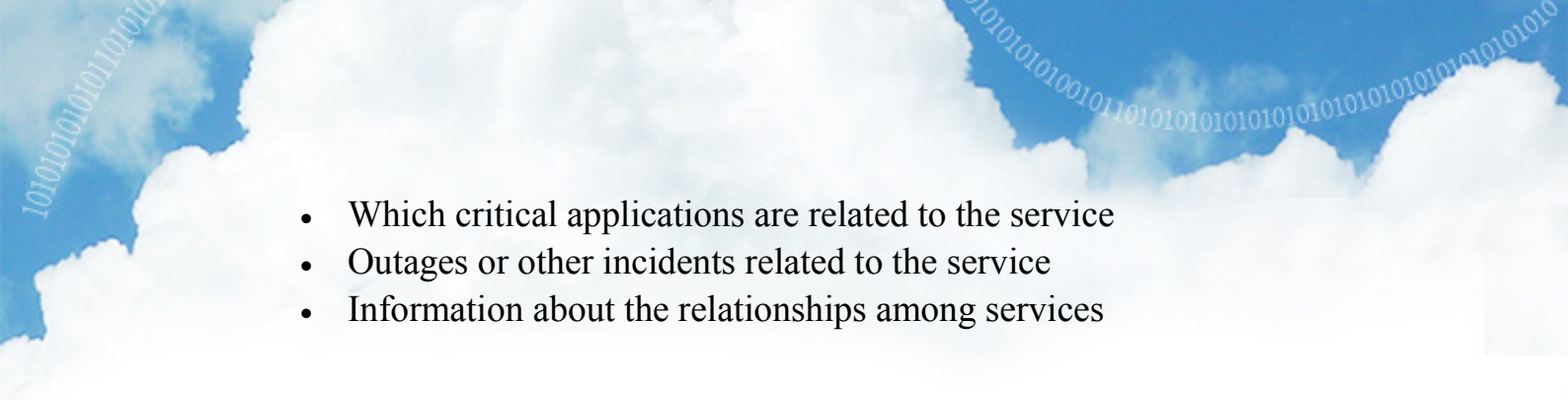
Build up Service Governance Strategies

Cloud service providers often offer a lot of service packages that users have to manage. An individual or group in the user's organisation is needed to deal with cloud issues and business processes around these issues. This individual or group should have oversight and collaborate with the business processes around cloud issues that directly impact the organisation. It can also develop best practices for managing cloud environments.

In addition to interacting with cloud service provider(s), users must also monitor what these cloud providers are doing. However, only a few emerging vendors provide tools, say dashboard interface, that enable users to monitor their cloud providers.

On the other hand, users should maintain service catalogue (a record of IT services) for cloud. The catalogue can include information such as

- Whom to contact about a service
- Who has authority to change the service

- 
- Which critical applications are related to the service
 - Outages or other incidents related to the service
 - Information about the relationships among services

Key Area 5: Security and Privacy Protections

Cloud computing can be viewed as an extended form of traditional outsourcing activity that involves the user organisation entrusting the hosting of its sensitive data to cloud service providers and the granting of network access by cloud service providers to that data. The security and privacy protection of the user organisation's sensitive data continues to remain a very important issue. With reference to various studies and research, security and privacy are cited by many organisations as the top inhibitors in the adoption of Cloud services. Some concerns are associated with the security level of services provided and other concerns relate to specific security requirements in data management and protection, access control and resiliency, etc. In general, to enable the partnership between the cloud user and the cloud service provider to continue successfully, both parties must stay vigilant to the risks involved so that they can be better prepared to circumvent or mitigate these risks. Both the user organisation and the cloud service provider need to clearly understand their respective roles and responsibilities when selecting, providing and using cloud services. When the risks are appropriately managed through the implementation of security measures, most of the security concerns of cloud computing can be mitigated.

In the cloud service business, the protection and privacy of the user organisation's sensitive data is a critical function that has increasingly become a key determinant of business success. Cloud service providers capable of demonstrating their ability to protect and continuously make available the consumer organisation's sensitive data entrusted to them can gain additional trust and confidence from their users.

Cloud users and SMEs need to understand and educate themselves with the changes in approach being applied to the processing of their data and maintain an in-depth understanding of the issues and concerns for ensuring the on-going protection of their data in the cloud services environment. The user organisation additionally needs to ensure they are knowledgeable, through verification steps, to ensure the adequacy of

the security controls adopted by the cloud service provider, to enable sufficient trust that the cloud service provider is capable of adequately protecting the user organisation's sensitive data.

To facilitate cloud user organisations in understanding the security issues on using cloud services and to assist cloud service providers in defining appropriate and relevant security controls, two checklists have been prepared by the Working Group on Cloud Security and Privacy established under the Expert Group on Cloud Computing Services and Standards. These two checklists are made available for free download from the Government's InfoCloud website.

URL for the Security Checklist for Cloud Service Consumers:

http://www.infocloud.gov.hk/themes/ogcio/media/featuredarticles/WGCS_P-4-6a_Security_Checklists_for_Cloud_Service_Consumers_EN.pdf

URL for the Security & Privacy Checklist for Cloud Service Providers in Handling Personal Identifiable Information in Cloud Platforms:

http://www.infocloud.gov.hk/themes/ogcio/media/featuredarticles/WGCS_P-5-4a_Security_and_Privacy_Checklist_for_CSPs_in_Handling_PII_in_Cloud_Platforms_EN.pdf

Key Area 6: Service Commitments / Warranties

Current Market Practice

A key part of any contract for cloud computing is going to be the commitments the service provider makes with respect to its service and the warranties that the service provider offers with respect to the performance. A service provider's failure to meet the commitments and warranties provided will give rise to certain remedies, therefore, service commitments should be:

- in the form of a clearly defined obligation
- clear as to any time or other limitations
- clear as to the remedy for failure to meet the commitment.

Current market practice is that service providers' standard service contracts will have very limited or no service commitments or warranties and that any service "guarantees" will be wrapped up in the service levels. Particularly with respect to commoditised cloud service offerings, service contract terms will not be negotiable and offered on a "take it or leave it" basis.

Standard Terms of Service

In many cases, particularly for standard offerings, cloud service agreements will be a set of standard terms which are favourable to the service provider and are not open to negotiation (see Key Area 9 "Contracting"). These standard terms will usually contain very limited service commitments and warranties and a set of limitations and exclusion of liability which further limit the service provider's obligations.

Where negotiation is not possible, a customer will need to determine

whether the service commitments match the service provider's representations and its own requirements, that any limitation on service provider liability are identified and understood and the appropriateness of the service offering is assessed.

Pre-contractual Statements

If any representations have been made to the customer by the service provider prior to the signing of the contract either in writing, verbally or through information made available about the service regarding service commitments and warranties, then these will need to be repeated in the contract document itself to be part of the contract. A common misconception by customers is that such pre-contractual representations will ultimately form part of the contract and will be able to be relied on if promises are not kept at a later stage. In fact, the opposite is often true in that the contract will expressly provide that any statement not recorded in the contract is excluded.

Matching the User's Requirements

The user will have undertaken a preliminary assessment to understand its practical and technical needs for the cloud service and any restrictions, limitations or regulatory requirements which may shape the type of service it requires. These requirements will often include:

- features of the cloud service;
- performance and service levels;
- data security;
- data location;
- service provider support; and
- end of contract data transition.

Each user's requirements will differ according to the nature of its data, its industry and any regulation and purpose for using the service. These

requirements will be more detailed if the user is trying to achieve a bespoke cloud solution rather than fitting a standardised offering to its needs.

Once the user understands its own requirements and sensitivities, it is important for the user to identify whether its requirements match the service commitments offered by the service provider in the service agreement. It is very common for service providers to provide only very limited service commitments and warranties and as will be discussed below, service agreements will often limit or disclaim the service provider's liability for the limited commitments that it has.

If a service provider is offering standard terms or is not showing much willingness to negotiate, the user will need to assess whether the commitments offered by the service provider will match its needs and, if not, consider either modifying its requirements or looking for another cloud solution.

Reading the Fine Print - Disclaimers

Disclaimers, limitations and exclusions of liability by service providers are key issues for users. As service providers will typically try to exclude or limit their exposure under a cloud service agreement, the exclusions or limitations will generally cut across or minimise the value of any commitments that a service provider was willing to offer. Such limitations of liability can limit monetary damages for which the service provider is liable, but liability for certain events or incidents can also be disclaimed. The exclusion of liability which generally causes the most concern for customers is for service outages and data loss.

Many cloud service providers will argue against negotiating variations to liability for commoditised services, the argument being that users cannot expect high levels of service provider's liability for low cost solutions. Users of more bespoke, higher cost services may have more leverage to expect more service provider liability and will often be more demanding with respect to service provider liability for matters such as data loss,

security breaches and breaches of confidentiality and data protection laws. This can be an area of lengthy discussion and negotiation.

Therefore, as part of assessing the commitments and warranties that a service provider is prepared to provide with respect to its services, a user should also ensure that it understands the limitations on those commitments.

Are the Commitments Appropriate?

Taking into account the user's own requirements, service commitments and warranties in the service agreement, limitations or disclaimers on those commitments and the ability (or not) to negotiate with a service provider, a user must weigh up the suitability of the cloud solution. Particularly when dealing with commoditised solutions, it may not be possible to "tick all the boxes" in terms of service commitments and liability. However, by understanding the offering and limitations, an informed decision can be made by a user as to whether the service offering is appropriate for its needs, whether it is willing to accept the risks that are not covered by the service provider or whether another solution and/or provider should be found.

Key Area 7: Data Ownership & Location and IP Ownership

Current Market Situation

Cloud services entail issues on data ownership and intellectual property (IP) similar to traditional IT outsourcing. Cloud services introduce additional issues on data location. The business nature of cloud services, be they IaaS, PaaS or SaaS, makes understanding where data is, who has access to it and how it is being used more difficult. This is due to a much higher degree of virtualisation and sharing in server, storage, network and applications. In general, cloud service providers may not clearly mention data ownership, data location and IP ownership of user data and application programs.

Key Points to Note

Data Ownership

- Users generally need to retain ownership of, and rights to use their data stored with cloud services. Users should find out from the service provider the ownership of their data (including application programs developed in the cloud and data created in the cloud) and what the service provider can do with the data. Users also need to understand what will happen to their data in the event that the service provider can no longer offer the services.
- Users should ask the service provider for any precautionary measures (e.g. data backup) to preserve and prevent any corruption or loss of their data. Users should also find out from the responsibilities of the service provider in recovering or restoration of their data in the event of any data corruption.

Data Location

- Often there is a reality of location independence in that users may have no control or knowledge over the exact location of the provided computing resources as a result of extensive virtualisation of computing resources, especially in a public cloud environment. Cloud service providers are more likely to use sub-contractors to meet spikes in demand. Cloud-stored data often transfers among various locations, sometimes from country to country. It may be difficult for users to control data movement and storage, causing enforcement of organisational data protection policies and standards difficult. Having said that, some service providers allow users to designate data location at a higher level of specification (e.g. country of data centre). Users should understand the whereabouts of their cloud-stored data and if necessary, to agree with the service provider on the data location. It is equally important for users to understand how the data is properly erased when the computing resources are de-provisioned.

Intellectual Property Rights (IPR)

- Apart from data, users may develop and run application systems in a cloud services. The user and the service provider should clearly agree in which party IPR will vest in data and application programs being developed through the cloud services.
- The user will eventually need to transit data and application programs from a cloud service provider to another provider or back to an in-house system upon contract expiry. These data and programs can be created or developed based on software (e.g. operating systems, application development tools) owned by the current cloud service provider. The user should agree with the service provider beforehand the scope of data and application programs that can be taken away at contract expiry.

Key Area 8: Service Default

Current Market Practice

A service default occurs when the cloud service provider fails to provide the services. This failure may or may not give rise to rights for the user, depending on the services agreement and the facts of the service default. The rights a user may have for a service default are typically some sort of damages, such as a refund of services fees or reperformance of the services.

In order for the user to have any rights in the case of service default, three things must exist:

- Obligation - the service provider must in fact have an actual obligation to provide the services;
- Not Excused - the service default must not be excused; and
- Extent of Rights - the rights must be allowed.

Each of these things will be provided for (to the extent they exist) through the cloud service agreement.

Overview

Before there can be a services default under a cloud services arrangement the service provider must have an obligation to perform the services in the first place. As discussed in a number of the Key Area topics of this Practice Guide, many times cloud services contracts carry few, if any, commitments by the provider to actually provide the services. Further, even where the service provider gives performance commitments, often such commitments are narrowly scoped or broadly excused. This is why it is very important for a user to understand what commitments the service provider is making and what rights it has if there is a service default before deciding if a particular cloud solution is one it can use in

its business.

Frequent Limited Reciprocal Obligations

As noted, in many cloud services arrangements the service provider makes few or no defined obligations to provide the services. In such a case, there is really no basis for a service default. Typically such a service arrangement would have similarly limited obligations on the user – most likely limited to pay if and to the extent services are received. In such a case, each of the service provider and the user can carry on as long as it perceives value in doing so and the other party remains willing.² Such an arrangement may be appropriate for non-business critical functions or data, but would present high risk to a user’s business if used for necessary functions or sensitive data.

On the other hand, some cloud service providers are willing to give some performance commitments knowing that this is likely necessary if it wants its services to be used in business contexts. In these situations, because the service provider has a commitment to perform, if it fails, a service default may occur. The services contract, in such a case, will provide the rights the user will have in case of such a failure to perform. The two classic rights (often referred to as “remedies”) for service default situations are the right of termination and the right to damages. Each of these will be discussed in turn.

Before addressing potential remedies for service default, it is important to consider that the service contract may provide that in certain cases the service provider’s failure to provide the services may be excused.

² Such corresponding ability to terminate is not always provided in service provider forms, and the customer must be satisfied that the obligations it takes on are acceptable in light of the commitments made by the service provider. See Key Area 9 for a discussion of formation of cloud services contracts and service contracts prepared by service providers with little or no room for negotiation on part of the customer.

Excused Non-Performance

It is common that contracts containing obligations to perform also contain specific provisions that excuse non-performance. A user must carefully consider any such contract provisions to determine if they raise unacceptable levels of risk for the user. One example of excused performance provisions, and probably the most common, applies in the context of a “force majeure” event.

A force majeure provision defines potentially events, which are typically acts of nature (floods, earthquakes) or other described events such as wars, revolution and the like, in each case not caused by the service provider and beyond its reasonable control. The provision defines the extent to which the service provider is excused from performance to the extent it is prevented from performing because of the event, including the point at which one or both the user and service provider have the right to terminate the contract if services have not been reinstated, whether or not the force majeure event continues, and the details associated with any such termination.

The other excused performance provision sometimes included in a services contract involves situations where the service provider is unable to perform because of something the user did (usually something negligent or wrong) or failed to do (usually something expressly required of the user under the contract). In many service contracts these are relatively detailed provisions and actively negotiated in view of the significant inter-dependencies and differing roles of the parties.

As noted, the user must carefully consider if these excused performance provisions are acceptable, or raise too much risk for the user to use the cloud service in its business operations.

Remedies

Where a services contract contains obligations requiring service provider

performance and a non-excused performance failure occurs, the user must again look to the contract for the user's rights resulting from the non-performance. The two most common rights are rights of termination and to damages.

Termination

Service agreements frequently contain provisions that allow the user expanded termination rights in the event of certain non-excused service defaults. Some provisions may be triggered simply by any non-excused default, but others apply with a “material” default or other expressly defined default circumstances (such accumulation of a certain volume of service level credits). The provisions may also require the user to give the service provider notice of the default and opportunity to cure it, if the default is one that the service provider can cure.

Two related considerations that the user may want to consider here are (i) its ability to exercise the right to terminate the contract less than entirely – that is, in part rather than in whole; and (ii) not having the exercise of a termination right be an exclusive remedy for the default. While the right to partially terminate may be less significant in cloud services arrangements where the scope of services often tends to be narrower than in other service agreements, the right of partial termination can be an important protection for the user.

As for the termination right serving as an exclusive remedy, if such is the case, the only thing the user can do is terminate the agreement, but not obtain any damages (potentially not even its money back) .

Damages and Limitation of Liability

The second remedy most commonly associated with service default is the right to damages. Damages typically represent monetary reimbursements for at least some of the losses resulting to the user from

the service provider's failure to provide the services.³ In this regard, it is standard industry practice for service agreements to include express provisions defining the extent of the service provider's potential liability under the services contract for service defaults. Frequently, these limits are expressed in terms of a total maximum amount (or amounts⁴) over the life of the contract or over defined periods, often expressed in terms of payments over a number of months under the agreement. These provisions may also limit the damages available to the user's immediate (sometimes referred to as "direct") damages, and excluding more "remote" damages, such as lost profits. This is one area where cloud service providers seem to have fully embraced concepts from traditional services arrangements – and most service provider agreements seek to provide such limitations. In fact, pure utility cloud arrangements frequently seek to disclaim most or even all potential liability.

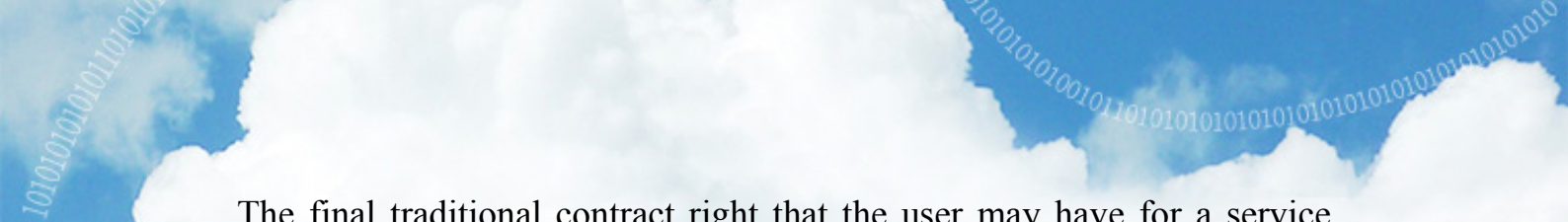
Depending on the nature of the service agreement and the negotiation of the parties, limitation of liability provisions can be detailed and is the subject of significant negotiation between the parties.⁵ This tends to be less the case especially with public cloud service arrangements where performance obligations are often less firm in the first place.

Specific performance

³ In some cases and contexts damages may be stipulated (pre-agreed) in terms of amount and these are referred to as liquidated damages. There are certain requirements for liquidated damages to be valid under law, including that they should represent a reasonable approximation of damage associated with a default and they frequently represent the exclusive (complete) damages associated with the default.

⁴ Service agreements may, for example, contain different caps for security and confidentiality breaches around personal data and other identified high risk areas for failed performance.

⁵ Beyond special service default exceptions to liability caps, it is common that service agreements contain exceptions for particularly egregious conduct, such as criminal, fraudulent or wilful misconduct or even gross negligence of service provider and its personnel. Even without such exceptions from otherwise applicable liability caps, such conduct often may not be subject to limitation of liability as a matter of public policy.

The header of the page features a blue sky with white clouds. A decorative border of binary code (0s and 1s) runs diagonally across the top corners.

The final traditional contract right that the user may have for a service default is specific performance. This remedy involves the user obtaining a court order requiring the service provider to perform its failed obligations under the contract. Such court orders are typically difficult to obtain and require that the user prove special showings of harm. Often the right specific performance is disclaimed entirely in cloud service agreements.

Conclusion

As with all contract provisions, all of the provisions dealing with service commitments, excuses from performance commitments and rights for unexcused service defaults, must be carefully considered in light of the use to which the user is considering putting the services. This effort to balance and evaluate can be one of the biggest challenges in considering a cloud solution.

Key Area 9: Contracting (Terms of Service)

Current Market Situation

The terms of any cloud computing solution must be embodied in some form of a contractual arrangement, otherwise the user cannot have confidence that they will be performed, even to the extent that the services should be viewed as provided at the discretion of the service provider. This may be adequate for certain purposes, but not for systems or data of any commercial or legal significance. A user must understand the commitments of the service provider to performance and confirm that these adequately meet the user's requirements. A user must similarly understand the commitments it is making with respect to its use of the cloud services. Probably no other aspect of cloud computing puts so much pressure on the user to exercise diligence, discipline and responsibility, and in some cases serious restraint, often in the face of what seem highly attractive solutions from functionality and cost perspectives.

Role of the Contract

The literal act of contracting for cloud services is often extremely simple – as simple as an on-line click of “Accept” to the service provider's terms. In other cases, cloud services may be contracted for pursuant to a traditional printed and signed agreement. However formed, the contract and the user's rights and obligations under it, and the alignment of these to the requirements of the user – are critical considerations in adopting any cloud computing solution.

In any transaction, the contract or agreement establishes the rules and commitments between the parties. If a commitment is not contained in a binding contract, as a general matter it should be assumed to be

non-existent⁶. The contract plays an especially pivotal role in service transactions (such as cloud computing) because there is no tangible product, to define the delivery. Further, delivery of services is typically done over time. Thus, the services contract must define both the services themselves and the commitment and responsibility of the service provider to perform them. All of the important cloud computing issues discussed in this Practice Guide (Key Areas 1 through 8) are ultimately determined by the terms contained in (or absent from) the contract.⁷

Contracting for Cloud Computing

Although the method of contracting is not itself a defining attribute of cloud computing, in keeping with the overall Internet empowered and automated nature of cloud computing, often contract formation is on-line with little or no direct personal interaction between the parties. Frequently this involves merely the opportunity for an on-line “Accept” of the terms offered by the service provider. In fact, the contracting process can be so simple that some users may not fully appreciate that they have actually contracted, and with very little understanding for the terms. Nonetheless, such a contract can be every bit as binding and defining an agreement as an actively negotiated, printed and manually signed contract – and this can be true even for cloud services that become an integral component of the user’s operations.

⁶ Although there are some circumstances where rights under a contract may be expanded (or narrowed) by matters outside of the contract (for example, by conduct of the parties, such as misleading representations, etc.), such circumstances and possibilities are usually difficult to establish and are beyond this discussion. Similarly, depending on the applicable jurisdiction, there may be some statutory protection, such as Hong Kong’s Control of Exemptions Ordinance (Cap 71) or Misrepresentation Ordinance (Cap 284), which may impose some limitations on standard terms, but invariably fails to offer a viable alternative to address inadequate contract terms.

⁷ This Key Area 9 discussion will focus specifically on the contracting for cloud computing, but it is critical to remember that all of the issues related to a specific cloud computing solution as addressed in the other Key Area discussions of this Practice Guide (from service description to warranties to service levels and termination) are embodied there.

Be mindful of the source

A preliminary consideration with any service provider-provided form, as the case with on-line cloud computing contracts, is the obvious but sometimes under-appreciated fact that the contract itself is the work product of the service provider and inevitably will largely reflect its interests. Some service providers have increasingly come to recognise that their users are appropriately focused on contract terms and will require certain contractual protections in order to be able to use the services in a business context. These service providers are building in some accommodations into their form contracts. Nonetheless, it is still common today that cloud computing contracts prepared by service providers are highly favourable to the service provider, frequently:

- providing few, if any, service provider's obligations around:
 - service levels;
 - responsibility for compliance with laws;
 - security standards or data protection; or
 - any kind of non-routine requirements;
- containing broad disclaimer of all or most liability; and
- preserving the right for the service provider to suspend, terminate or change the services

Some of the more extreme service provider-oriented terms can constitute little more than a collection of disclaimers, subject to the user's obligation to make payment.

Further, some newer cloud service providers have little experience contracting for services and emphasise low cost, standardised offerings, with little room for robust contractual commitments, or user requirements. Actual negotiation of terms by a user may be extremely difficult (if not impossible), and if possible, may impact the service provider's ability to perform as part of a common solution offered across the service provider's customer base, thereby having both an adverse impact on

performance and costs.

From a theoretical perspective, there is rarely anything inherently wrong in and of itself with a particular contractual position staked out by a service provider in its form of contract. Rather, the risk from the user's perspective arises where there is misalignment between what the service provider contract is offering and what the user requires for the services and other commitments of the service provider, including misalignment that may arise over the course of the contract. This is especially true where critical functions or sensitive data are involved, which often presents compliance risks, such as concerns around data privacy and security and business continuity. These are risks the user retains in all events, and thus it is the user that must undertake the critical assessment to determine whether there is alignment between the offered and available contract terms and its specific requirements.

The conclusion reached by the user in its analysis of contract terms and its user requirements may often not be a simple go / no-go determination, but may involve a range of possibilities, including:

- the cloud solution is appropriate for adoption, but only for a limited range or purposes or uses within the user's organisation in order to avoid or mitigate unacceptable risks;
- the cloud solution is appropriate for adoption, but only in conjunction with the development and maintenance of internal procedures, practices or arrangements needed to mitigate risks (for example, development of a business continuity strategy beyond the solution, in case solution or its terms become unacceptable); or
- the cloud solution may be entirely inappropriate for adoption within the user's organisation.

Further, these decisions and their implementation often must be made (and maintained and monitored, and modified, as appropriate) within highly dynamic contexts, where both the user organisation and the cloud solution may change and there may be pressure within the organisation to take the solution beyond its appropriate bounds of use within the business.

Steps for Contracting for Cloud Computing Services

Responsible contracting for cloud computing solution requires the user to undertake a number of distinct steps, each of which must be tailored appropriately for the particular case:

Step One: User Requirements – data, applications and business needs

As a preliminary assessment, the cloud computing solution under consideration should be evaluated at a high level for elements or considerations that raise particular issues of concern. In short, some solutions may warrant and require detailed, in-depth assessment and consideration and others may not. This assessment should begin with a realistic appraisal of how the cloud solution will be used within the user organisation and the nature of the data involved. Although the specific considerations will vary in each case, the following is illustrative:



Through this assessment a determination can be developed regarding the various requirements of the cloud solution, including such aspects as reliability / availability, data control and security.

Step Two: Available Contract Terms (and Options)

Next, the user must develop a clear understanding of what the proposed terms are for the solution, including any optional terms provided by the service provider. Although it may seem as if this should be a straight forward undertaking, determining the actual terms for on-line contractual arrangements is not always easy. Often on-line contracts consist of a variety of documents containing inter-document links, which must be identified and tracked. It is important to obtain a clear understanding of all documents, terms, policies, terms behind active links and similar incorporated terms that are to form part of the contract between the service provider and the user. Also, there should be clarity of precedence in the event of conflicts between these various documents.

Although many cloud service providers may not be in a position or willing to negotiate, some are able to do so and it is at this point that the user would undertake negotiations with the service provider and seek to agree on terms that meet its requirements, to the extent possible. In such circumstances, the user may prefer to work with its form of agreement, but whichever party's form is used as the base for negotiation, the obvious objective of the parties is to reach agreement on what the user requires and the service provider is willing and able to provide.

Step Three: Assess Alignment of User Requirements and Available Contract Terms

Once a comprehensive determination has been made of the requirements and the terms of cloud computing service under the contract (whether standard offering or including some negotiation to address user needs), an assessment of the alignment (acceptability) from the user's perspective must be made. The conclusion here may be a definitive go or no-go, but frequently may be a qualified determination, involving the identification of risks, and approval based on limitations or arrangements to take risk to an acceptable level, as noted previously.

Step Four: Special Risk Consideration – Variable Terms

In cloud computing, there is a further contracting complication that often arises, particularly in the public utility cloud context and sometimes other cloud solutions—the reserved right of the service provider to unilaterally

modify the terms of services. Given the on-line nature of cloud computing and much of the contracting process, with some regularity cloud service providers seek to reserve the right to unilaterally vary the terms of service applicable to its solutions. A common method for this is the incorporation of terms by reference through description or web links, which are subject to continuous change by service provider. Such a right of unilateral change by the service provider renders the best planned and undertaken risk assessment and mitigation plan vulnerable to future changes in the services or other service provider commitments unilaterally imposed by the service provider and must be appreciated as a risk item.

If the cloud solution under consideration is of any meaningful business significance, there must be some method of mitigating risk of unilateral service provider changes, even if limited to a service provider commitment to provide pre-change notice and a right for the user to terminate at no charge or break fee if it finds the unilateral change unacceptable. However, even with this assurance (which itself must be embodied in the contract), the user must establish and maintain adequate contingency arrangements so that it can replace the cloud solution should unacceptable changes come to pass. This may necessitate a variety of arrangements, including retention of staff familiar with an area of work or permitting only limited adoption of the solution within the business.

Step Five: Traditional Service Provider Due Diligence

Beyond the foregoing steps, all of the traditional technology supplier due diligence should be undertaken to the satisfaction of the user. Although similar to any service provider due diligence, due diligence on a cloud service provider can present unique challenges, driven by the fundamental cloud computing reality that the processing facilities, as well data and software are beyond the physical control of the user.

The kinds of information relevant in a service provider due diligence investigation may include:

- reputation and reliability – references, third party assessments, certifications, case studies?

- user base – how many; service provider sponsored or independent user groups?
- service provider related physical location – address, telephone number.
- service provider management, experience and background.
- what kind of company – public, start-up, where does this organisation fit within the overall structure; credible investors; financial stability?
- active in social media sites, technical blogs?
- transparency – publish on public site outages, system issues fully disclosing?
- visibility into operational structure (subcontractors, third party participants in solution, etc.).
- business continuity, contingency planning, etc.

Conclusion

Contracting for services has always risen for any user. Cloud computing raises challenges because the attractive opportunities of cost savings and flexibility may lead to quick business decisions. Users must exercise discipline to manage their risk and the user alone can effectively undertake the requisite assessment and determination. Users should establish clear internal rules for cloud contracting to guard against unwittingly making bad tradeoffs between the tremendous promise of cloud computing such as cost savings and flexibility, versus risk.

References

- CIO Council and Chief Acquisition Officers Council. (2012). *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*. Retrieved on 28 December 2012, from <https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf>
- Cloud Computing Use Case Discussion Group. (2010). *Cloud Computing Use Cases*. Retrieved on 16 January 2013, from http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf
- Cloud Standards Customer Council. (2011). *Cloud Computing Use Cases Version 1.0*. Retrieved on 28 February 2013, from <http://www.cloudstandardscustomercouncil.org/use-cases/CloudComputingUseCases.pdf>
- Computer Associates (2008). *Virtualization Best Practices*. Retrieved on 28 December 2012, from http://supportconnectw.ca.com/public/impcd/r11/virtualization/doc/virtualization_best%20practices.pdf
- Department of Finance and Deregulation, Australian Government Information Management Office, *Negotiating the Cloud - Legal Issues in Cloud Computing*. Retrieved from <http://agimo.govspace.gov.au/files/2011/11/Cloud-Legal-Draft-Better-Practice-Guide-November-2011.pdf>
- DeveloperWorks Cloud Computing Editors IBM. (2010). *Review and Summary of Cloud Service Level Agreements*. Retrieved on 14 January 2013, from <http://www.ibm.com/developerworks/cloud/library/cl-rev2sla-pdf.pdf>
- Digital Inspiration. (2013). *Legal Issues around Cloud Computing*. Retrieved from <http://www.labnol.org/internet/cloud-computing-legal-issues/14120/>
- IBM Corporation. (2010). *Review and summary of cloud service level agreements from "Cloud Computing Use Cases Whitepaper" Version 4.0*, Retrieved on 16 January 2013, from <http://www.ibm.com/developerworks/cloud/library/cl-rev2sla-pdf.pdf>
- Information-technology Promotion Agency, Japan (IPA). (2011). *Guide to Safe Use of Cloud Services for Small-to-Mid-Sized Enterprises*. Retrieved on 28 December 2012, from http://www.ipa.go.jp/security/english/cloud/Cloud_tebiki_V1_ENG.pdf

- Institute of IT Professionals NZ Inc. (2012). *New Zealand Cloud Computing Code of Practice*, from <http://www.nzcloudcode.org.nz/wp-content/uploads/2012/05/NZCloudCode.pdf>
- Intel. (2010). *Intel® Cloud Builders Guide for Cloud On-Boarding with Citrix OpenCloud*. Retrieved on 28 February 2013, from http://software.intel.com/sites/default/files/m/c/5/1/a/0/31983-324432-001US_Citrix_Secure_d2.pdf
- Jinesh Varia. (2010). *Architecting for the Cloud: Best Practices*. Amazon Web Services, Retrieved on 14 January 2013, from <http://jineshvaria.s3.amazonaws.com/public/cloudbestpractices-jvaria.pdf>
- Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper. (2009). *Cloud Computing For Dummies*, Wiley
- Jurriaan Kamer, Harald Vranken. (2011). *The Impact Of Server Virtualization On ITIL Processes*, 1st International Conference on Cloud Computing and Services Science, CLOSER 2011, Retrieved on 18 January 2013, from http://kajurria.nl/Impact_of_Server_Virtualization_on_ITIL_Processes.pdf
- Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann, Jian Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf. (2011). *US Government Cloud Computing Technology Roadmap Volume II Useful Information for Cloud Adopters*, National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved on 31 December 2012, from http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf
- Malcom Fry. (2010). *IT Service Management (ITSM) And Cloud Computing*. Retrieved on 31 December 2012, from http://www.itsmf.cz/uws_files/odborne_clanky/itsm-cloud-computing-wp.pdf
- Mary Brandel. (2009). *Cloud computing: Don't get caught without an exit strategy*. Computerworld. Retrieved on 14 January 2013, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128665&source=NLT_AM
- NIST SAJACC and BUC Working Groups. (2011). *US Government Cloud Computing Technology Roadmap Volume III Technical Considerations for USG Cloud Computing Deployment Decisions*, National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved on 31 December 2012, from

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/RoadmapVolumeIIIWorkingDraft>

- North Carolina Department of Cultural Resources, Division of Archives and Records. (2012). *Best Practices for Cloud Computing, Records Management Considerations Version 1.0*. Retrieved on 14 January 2013, from http://www.records.ncdcr.gov/guides/cloud_computing_final_20120801.pdf
- Peter Mell, Timothy Grance. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved on 31 December 2012, from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina. (2009). *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*, in CCSW'09, November 13, 2009, Chicago, Illinois, USA. PARC and Fujitsu Laboratories of America. Retrieved on 14 January 2013, from <http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf>
- RightScale, Inc.. (2013). *RightScale Public Cloud Cost Calculator*, from <http://www.rightscale.com/cloud-cost-calculator/>
- Sharam Sasson. (2009). *Seven Best Practices for Cloud Computing*. Retrieved on 14 January 2013, from <http://esj.com/articles/2009/08/18/cloud-best-practices.aspx>
- Vivek Kundra. (2010). *State of Public Sector Cloud Computing*, CIO Council. Retrieved on 31 December 2012, from <https://cio.gov/wp-content/uploads/downloads/2012/09/StateOfCloudComputingReport-FINAL.pdf>
- Wayne Jansen, Timothy Grance. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology, US Department of Commerce. Retrieved on 31 December 2012, from <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>

FOR FURTHER INFORMATION, PLEASE VISIT OUR WEBSITE:

www.infocloud.gov.hk

InfoCloud website is established by the Expert Group on Cloud Computing Services and Standards. It serves as a one-stop portal for the general public and enterprises (especially SMEs) to effectively access information and resources on cloud computing technologies. The website provides sample use cases, guidelines and best practices for achieving the desired benefits in adopting the cloud computing model.

The Office of the Government Chief Information Officer of the Government established the Expert Group with an aim to draw expertise from the industry, academia, professional bodies and the Government to drive cloud computing adoption and deployment in Hong Kong, as well as facilitate exchanges among cloud experts both within Hong Kong and with the Mainland. Working Group on Provision and Use of Cloud Services is one of the working groups set up under the Expert Group.

This document is one of its series of best practices and guidelines prepared by the Working Group on Provision and Use of Cloud Services regarding the use of cloud computing and services. With the collaborative efforts from members of the Working Group, deliverables are developed with a view to facilitating and promoting wider adoption of cloud computing and use of cloud services in local industry.