WHITE PAPER: ITSM AND CLOUD COMPUTING

5 questions about ITSM and cloud computing

October 2010

Malcom Fry

AWARD-WINNING IT SERVICE MANAGEMENT EXPERT

we can

ca technologies

Table of Contents

What is the impact of the cloud on IT Service Management (ITSM)?

Cloud computing fits the typical modus operandi of emerging technologies in it is not new at all, but has progressed and matured into a viable, accessible, and cost-effective IT resource. Cloud computing has been used by most organizations for a long time, especially those organizations that use the open internet—it can be argued that the internet itself is a version of cloud computing. Once an organization adopts cloud computing it quickly becomes apparent that the traditional approach to IT service management needs to be reviewed. For example, who manages changes to the cloud, the cloud supplier or local IT? And how do the cloud suppliers notify their customers of scheduled changes? Failure to change traditional IT principles and approaches when adopting a cloud service will greatly increase the chances of failure. But, as opposed to locally managed services or outsourced services, reversing back to a previous status is much more difficult. It is like the difference between a flesh wound and a psychological problem; a flesh wound can be seen and easily treated, whereas a psychological illness may not been seen, is hard to determine and cure. It is the difference between what you own and control as opposed to the invisible and remote.

Cloud attributes

One of the key reasons why many organizations choose cloud computing is to better manage their costs and, in many cases, reduce their costs or see massive variations in costs. Cost savings are usually experienced in the area of capital expenditure savings items such as hardware, software, and services because they pay a supplier only for what they consume. Revenue can be saved due to better license management (e.g. if an organization has 1000 users who could be using a tool at the same time you would probably need 1000 licenses for that tool, but if you had a Pay-as-You-Go or Software-as-a-Service agreement then you would only pay for the number of users utilizing the service at a given time rather than pay for all 1000). This could represent a considerable savings. As the cloud progresses it could be akin to deregulation in the power industry, where you buy your services through a supplier who can provide a variety of sources. For example, in the UK you can get your electricity, gas, telephone, television, and broadband from one supplier for a monthly fee.

The most widely used definitions for cloud computing are supplied by the National Institute of Standards and Technology (NIST). The NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Essential Characteristics as defined by NIST:

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

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

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

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

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

National Institute of Standards and Technology - www.nist.gov

Maintenance is an ongoing issue for many IT organizations, especially upgrades to laptops or desktops and to extensively distributed software. With cloud computing you can have your software resident in the cloud, so when users start applications on their devices these programs are loaded directly from the cloud and not from a hard drive or a local server. This means that when the software on the cloud is updated, the new or updated version will be instantly available to all of the users without the need for complicated release and distribution plans.

One of the enduring and earliest attributes of cloud computing has been device and location independence, which provide users with access to services using a web browser irrespective of their location or indeed the device that they are using (e.g. smart phone or a laptop). This represented a significant change in the world of IT because for the first time a significant portion of the infrastructure was now resident but it had the advantage of allowing users to connect from anywhere.

With technology in a constant state of change it is important to quickly and inexpensively re-provision technological infrastructure resources. For example, if an organization decides to change smart phone suppliers this can be achieved in a cloud environment with very little effort, whereas in a less agile environment this could be a major undertaking. In fact there is no reason why you cannot have numerous smart phone suppliers, which, in a worldwide corporation, is a great advantage.

Scalability has always been a thorn in the side of IT, especially those with seasonal or other on-demand spikes. Using concepts such as distributed data grids within cloud scalability ceases to be a problem when you have to provide that capacity from local resources. In addition it is easier to meet the scalability that can be attributed to growth (e.g., if the organization headcount increases by 500 people the cloud would be able handle this new workload).

There are many more cloud computing attributes that are interesting to explore and discuss, including multi-tenancy, reliability, and sustainability. A small amount of research shows the power and flexibility of cloud computing, but what it doesn't often highlight is how IT needs to change the way service management operates if it is to fully benefit from the attributes that can be attributed to cloud computing.

There is no doubt that cloud computing has many valuable attributes and is becoming a vital resource for many organizations, but this should not obscure the fact that there are risks that need to be addressed.

Deployment models of cloud formations

Cloud formations can have numerous variations and mutations, but for conversational purposes they can be grouped into four categories: public clouds (also known as external clouds), community clouds, private clouds (also known as internal clouds), and hybrid clouds. Public clouds have been around for a long time and as such are a familiar technology resource that provides web applications and services via the Internet using remote third-party suppliers.

Deployment Models as defined by NIST:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

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

National Institute of Standards and Technology - www.nist.gov

A community cloud is a viable option when numerous organizations have similar industry-related technology requirements, resulting in them wishing to share a cloud infrastructure and, as a result, gaining some of the benefits of cloud computing across a common scenario. Adopting this approach can be more expensive than utilizing public clouds because some bespoke development activity could be required. However, on a positive note, it may offer higher levels of privacy, security, and/or governance than a public

cloud. Community clouds are often industry-based, with a good example being Google's government cloud designed especially for US Government agencies.

In simple terms, private clouds can be described as services that provide cloud computing on private networks. The intention is to reduce some of the potential pitfalls that can occur when using community and public clouds, specifically" data security, governance, and reliability. However, private clouds are usually more expensive because they have to be built and managed independently.

The last formation is the hybrid cloud environment, which comprises multiple internal and/or external cloud suppliers (e.g., a public cloud could be used to provide services to a private cloud).

There is one common thread that is often overlooked when embracing cloud computing and that is if cloud computing is to deliver on its promise that *you need technology to manage technology,* old traditional methods of managing services will not be able to cope.

Service models

If there is one area of cloud computing that is sure to create conversation and divide opinions it is the subject of cloud service models. Although it is generally accepted that there are only three main variants, each of these can sub-divide into many numerous variants.

Service Models as defined by NIST:

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

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

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

National Institute of Standards and Technology - www.nist.gov

If you read the NIST definition of the cloud service models you will notice that there is one consistent phrase that appears in each model: "the consumer does not manage or control." And it is in these words where the controversy often lies. The argument is that the less you control, the more vulnerable you are to security threats, performance issues, change failures, compatibility concerns, etc. However, these same arguments were addressed successfully by outsourcing and they are being addressed by cloud computing organizations. The real secret of success lies in two factors: choosing the correct model and performing detailed preparation before a model is adopted. Choosing the correct model is a strategy level decision that requires clear and unequivocal information and knowledge, which is why the service portfolio is so important at this stage. There is an old adage—the better informed you are the more likely you will make the correct decision. It certainly applies here. This is not a decision to rush.

The relationship between ITSM and cloud computing

According to the Information Technology Infrastructure Library (ITIL®) there are four phases in the lifecycle of a service or application: service strategy design, service transition, service operation, and continual service improvement. The four lifecycle phases are more critical for cloud computing than they are for traditional computing because most of the activity occurs remotely, which reduces the amount of control that can be levered locally and leads to problems, unexpected outages or unmet expectations. For example, should the cloud supplier include their customers in their change management process? If not, who is culpable if a change fails causing an outage? Or what happens if the workload demand is wrongly calculated? Could this lead to unexpected costs being incurred?

Successful cloud computing starts with careful strategic planning to decide which service strategy to adopt (e.g. to utilize cloud computing as a strategy to improve a current service or to implement a new service). From the service management viewpoint this encompasses portfolio management, demand management, and financial management. Portfolio management provides a description of the cloud candidate, while demand management calculates the workload and financial management calculates the costs required to supply and meet the workload demands. If these calculations are inaccurate or ignored then not only could the wrong delivery service be selected but also the incorrect charging algorithm could be adopted. Service strategy is essential because it is the foundation stone for cloud computing.

Once a strategy has been adopted then the next step must be to design the service that will best deliver that strategy. It is important to understand that when services are delivered from a distance (e.g. cloud computing), specifying and designing the service are vital because errors can be costly and slow to correct, especially if binding contracts are to be signed. Service levels need to be prepared and agreed upon so all parties understand their deliverables and properly set expectations; ideally the Service Level Agreement (SLA)s should be included in cloud contracts. Availability and capacity analysis and calculations are to be performed to ensure that the services described in the portfolio and specified in the SLAs can be delivered by cloud computing suppliers. Remember you can abdicate responsibility, but you cannot abdicate accountability. So although the external cloud supplier may be directed to meet the SLA targets, IT is accountable for failed or poor SLAs. The essential back office functions concerning IT service continuity management and information security management have to be in place before the service enters the live

environment. Suppliers have to be identified and selected. All of these activities are part of service design. Missing any of these components or getting any of them wrong can have disastrous results for cloud computing (e.g., do the cloud computing suppliers have proven continuity management and do contracts with suppliers meet international standards).

With the strategy in place and the design complete, the next step for a service or application is the transition from preproduction into to the live environment. ITIL calls this stage service transition, which is appropriate because it involves far more than change management. It is now with change management that the union between in-house technologies and cloud technologies fuse for the first time. It is also where the first potential flashpoint occurs—who owns change management at this point? IT or the cloud suppliers? And who will own and manage changes in the future? Change ownership and relationships are vital to establish before transition into production status. As the service is rolled out then release and deployment management is required to ensure the rollout is successful and well managed because the less in-house technology employed the more there will be issues such as release versions of software and the updating of remote technologies and smart phones. Underpinning service transition are service asset and configuration management, which will detail exactly who owns the responsibility for the devices and software required to provide the new service, as well as the configuration management system where those assets reside. Service transition is the last-chance saloon because errors here can be extremely difficult and expensive to resolve once in production.

Once a service is in operation in the cloud it has to be carefully monitored to ensure that it delivers the levels of service defined in the contracts and specified in the SLAs. This will require external cloud consumers to have access to the raw data collected by the cloud supplier. Typically, in ITIL, this would include analyzing incidents that have been recorded by the service desk. But if the service resides in the cloud, where is the service desk, who owns it, and how do the customers contact it? The role and ownership of any service desk or other support points must be clearly defined and monitored. Traditionally IT service desks have concentrated on high performance levels, such as high first level incident solving rates, but with cloud computing the emphasis must be on identifying the root causes of incidents and then eliminating them using problem management—rather than applying workarounds otherwise the benefits of the cloud will be reduced. Another key component in service operation is access management because constant vigilance must be maintained to ensure nobody breaches cloud security measures.

To get the best from cloud computing it is advisable to adopt established best practices rather than to trust organic home grown practices. It is generally accepted that ITIL is the leading best practice for service management, while COBIT is the leading best practice for quality control and assurance for IT service management. ITIL and COBIT have been designed to work in tandem and provide a tried and trusted solution. The highest level of attainment for IT service management is ISO 20000, but without best practices in place ISO 20000 is very difficult to obtain.

The last word

Just to show how unpredictable the cloud can be, here is an interesting example concerning an extradition case involving the US and the UK in which the US is waiting for Gary McKinnon to be extradited for the crime of hacking into US military computers. (Refer to the Gary McKinnon blog for more information: http://connecttheworld.blogs.cnn.com/2010/03/25/mondays-connector-janis-sharp/?iref=allsearch). The point here is that he was physically in the UK but used the cloud to commit the crime against the US government. He has admitted to the crime, but where should he be tried? Should it be in the UK where he perpetrated the crime or in the US where the impact of the crime occurred? This could have important implications for cloud computing because if the extradition is successful then we have someone being prosecuted for the crime at the virtual rather than physical location of the crime. If this extradition goes ahead then a new precedent could be set in law. For example, in the future, if a US citizen living in the US commits an internet crime and steals money from a UK bank, where should that person be prosecuted? In the US where the crime was committed or in the UK where the impact of the crime occurred? Just a thought.

How does service strategy work with cloud computing?

In most organizations, IT service management has been seen more as a back-office function that is by nature an operational function rather than a strategic resource. For those large organizations with large investments in IT resources, this may still be the case. More pioneering organizations have found that ITSM is a vital function to obtaining the best results possible from external cloud computing. Using the NIST definition, external cloud computing would include the community cloud, public cloud, and hybrid cloud.

ITIL is the most widely used best practice in IT service management. It is based around a lifecycle approach to service management and can provide great support to organizations in reducing risk and gaining maximum benefit from cloud computing. This includes both internal and external cloud deployments and service models (as defined by NIST), especially in the areas of service strategy. ITIL service strategy has three components that must be applied to reducing risks and maximizing benefits for external cloud computing: portfolio management, demand management, and financial management.

To select the correct cloud service model formation, and to decide upon the most advantageous external cloud deployment model (NIST definition), it is vital that the decision makers fully understand the applications and services they are evaluating as potential candidates for cloud computing. It is for this reason that portfolio management is so important. The main portfolio management constituents are service, project, and application. These jointly provide the information to ensure that the correct external cloud model is selected. Not only does portfolio management contain all of the information to ensure successful adoption of cloud computing, it also provides a common central repository of information,

accessible by all parties focusing on cloud adoption, including cloud suppliers and cloud consumers. It is essential that a portfolio be created for all potential external cloud deployment models. Without portfolio management providing a central description of the service, it is extremely difficult to bring together the needs and requirements of the diverse IT departments who will need to be involved for external cloud computing.

Demand management calculates and coordinates with the consumers the usage demand on a service. This will ensure appropriate levels of resources will be available for every service. For non-cloud services, this is not too much of an issue because it is fairly easy to increase capacity if at a later date demand has been calculated incorrectly. But with cloud, an error in calculating demand could prove very costly, especially if you have a service-on-demand agreement with an agreed level of capacity. In this instance, the chance is that any usage over the agreed levels will be charged at a premium rate. Just as a pay-as-you-go cell phone plan initially seems like a bargain, heavy usage suddenly becomes very expensive. Demand management must carefully calculate demand to ensure there are no nasty surprises.

Financial management affects not just IT service management but all areas of IT and has in-depth knowledge concerning current costs, budgets, and charges. Many cloud services are justified because of their ability to save costs over more traditional areas of IT, but is this really true or is it a vacuous claim? This claim can only be decided by financial management having an in-depth knowledge of current costs and charges so that these can then be compared with the projected charges for potential cloud services. For example, consumers must know their current cost structure and unit of cost measurement (i.e., an exchange mailbox cost them $40.00 per month per user), otherwise how will they know whether a cloud supplier is competitive or not? Consumer financial managers must carefully calculate, along with the users of the service, the potential costs of a new service to ensure they will indeed provide measurable cost savings.

Service strategy questions

PORTFOLIO MANAGEMENT

- Has the service or application been clearly specified so all parties understand their roles and responsibilities? Special consideration needs to be given as to whether the cloud has been correctly identified as the appropriate delivery vehicle. Where is it as part of the overall computing strategy for delivery of service?
  - > *Failure to clearly specify the delivery model could result in service delays when fixing incidents and problems.*
- Has a service portfolio been prepared for the new service or application and have the cloud suppliers seen and agreed upon the service portfolio for each service or application?
  - > *The service portfolio is used to manage the complete service cycle. Failure to have a managed service portfolio will result in problems synchronizing between the various resources working to employ cloud computing. If the cloud suppliers have not seen and agreed upon the service portfolio then there could be potential contract disputes in the future.*

DEMAND MANAGEMENT

- Has the demand for cloud services been accurately calculated, especially the demand for peak periods and predictable highs and lows, including establishing the authorization processes are in place to accept spending for additional capacity?
  - > *Failure to calculate the demand accurately could result in agreed demand levels being exceeded and penalties being levied by the cloud suppliers.*
- Have the performance requirements for cloud services been accurately specified, especially the performance required for peak periods and predictable highs and lows?
  - > *Performance is increasingly important especially if remote devices, such as smart phones, are to be employed. Failure to calculate and specify performance could lead to frustrating delays for users of cloud-based services.*

FINANCIAL MANAGEMENT

- If financial savings are one of the reasons that a cloud service model (NIST definition) has been chosen, then have the costs for the outgoing service delivery agent (e.g. in-house) been accurately calculated so that true savings can be identified?
  - > *If these cost structure s are not in place then the true savings of cloud computing cannot be calculated. Without this data cloud computing could be an expensive alternative.*
- Is the cloud supplier going to provide visualization for costs to be observed and checked if they approach or exceed agreed-upon financial limits?
  - > *Without visualization, costing feedback will have to be on a periodic basis which can mean higher costs if over-usage is left uncontrolled for a period of time.*

Summary

Like any job well done, success is often dependent upon the quality of the preparation. Failure to prepare properly will eventually cause problems. Sometimes service strategy seems like overkill, but if you are relinquishing control to an external resource, then overkill is a better policy than being unprepared. Otherwise, the implications can be very painful. Risk management and risk assessment are the key elements. This is because risks do not just result in higher costs, but also include impact of failures on the organization, as well as the services and products they supply to their customers. There are many potential implications linked to the failure to perform diligent service strategy when selecting external cloud services:

- Demand is exceeded, resulting in higher costs
- Cloud may not be the correct delivery vehicle for an application
- Once a cloud service has been implemented, it is difficult to bring back in-house
- Local expertise is lost due to lack of planning or due to staff repurposing
- Users can become more skilled with the cloud service than IT because IT may not use the product which can make life very difficult for the service desk and change management

- Scope and limits of the cloud service may not be understood
- A traditional approach may be cheaper and more efficient that the proposed cloud service

Performing diligent service strategy will reduce the possibility of adopting an approach that is new wave, trendy, or just presents an interesting challenge. Service strategy expects all potential delivery vehicles to be evaluated as part of strategy generation. Adopting an external cloud is a business decision, not just an IT directive. As a result, consumer business managers need the involvement that performing service strategy demands. Failure to recognize the role of business managers in service strategy could result in adopting a solution that hinders rather than enhances business services.

How does service design work with cloud computing?

ITIL is the most widely used best practice in IT Service Management. It is based around a lifecycle approach to service management and can provide great support to organizations in reducing risk and gaining maximum benefit from cloud computing. This includes both internal and external cloud service and deployment models, especially in the areas of service design, which is a key component in the planning phase for the adoption of new services and applications. It is guided by the portfolio created by portfolio management. Key processes in service design for external cloud computing include: availability management, capacity management, service continuity management, information security management, supplier (provider) management, service catalog management and service level management. Many of these processes wear two hats, the first being calculating the requirements and the second being the measuring and monitoring of the service. For example, capacity has to be calculated and commissioned for new services, but once the service is implemented, the capacity has to be measured on a continual basis.

One of the most significant advantages of external cloud computing is that it can eliminate many of the issues associated with availability management. This is because this delivery model is not constrained by local concerns such as staffing and local technology resources. There is a danger that the cloud can create an aura of complacency, however, when dealing with cloud computing. Some of the external cloud computing charges can be based upon availability. As a result, it is important that availability management is responsible to carefully calculate the availability requirements for all applications and services that will utilize the cloud. In addition, availability management should install measurement tools to monitor usage to ensure that availability levels are maintained within acceptable and agreed levels. This advantage can be negated if availability requirements are badly identified, resulting in availability being required outside the agreed contract boundaries resulting in unplanned charges from the cloud supplier.

The criterion for capacity management is the same as for availability management because they need to be calculated and monitored. It is important that regular analysis is performed to ensure that capacity levels are meeting planned growth expectations. If this analysis is not performed, it is possible that capacity will exceed the levels contracted with the cloud suppliers and, as a result, the supplier could incur financial penalties.

As technology penetrates further and further into the fabric of an organization, so does the need for continuity planning increase. When all technology resources are in-house, continuity is a local administrative activity, but the moment that an organization uses an external IT resource such as cloud computing, the situation becomes more complex. Service continuity should be charged with identifying the exact service continuity requirements for external cloud computing and making sure that these are contracted with the external cloud supplier and regularly checked and updated when necessary.

Security is an obvious and the primary concern for all organizations utilizing cloud computing. The levels of concern differ widely depending upon the services that are processed by cloud computing. For example, usage for services such as calendars and email will need some level of security—but nothing like the security levels required for sensitive data stored in the external cloud. This is why information security management plays such a key role in external cloud computing. With security, the concept is to anticipate as many potential threats as possible and put safeguards in place to prevent security breaches. Information security management should also diligently monitor for any breaches in external cloud computing services and applications.

Supplier management and cloud computing often have a slightly strange relationship because many of the cloud services can be contracted online without the traditional meetings and negotiations. This removes a level of communication, and makes it necessary for very careful inspection of external cloud computing contracts before they are signed. Careful measurements of the terms in the contract are needed to ensure they meet the exact contractual obligations. Another aspect to keep in mind is what constitutes a legal contract in one country may not be deemed legal in another country. The source of any contract signed for external cloud computing services should be determined to verify the validity of the contract. These vital functions are provided by supplier management.

Service Catalog Management is one of the more obvious components required when managing cloud computing because it contains much of the criteria that govern how service support components function as this quote from the ITIL Service Design book explains; "*the Service Management Process is to ensure that a service catalog is produced and maintained, containing accurate information on all operational services and those being prepared to run operationally*". The key here is 'all operational services' which will include both cloud services and other operational services such as internal services and outsourced services. The Service Catalog is the only place where all of these services, and the relationships between them, are viewed from a single point of observation to ensure that the correct services are provided to the appropriate IT customers. When all services are provided internally this is an important but not a critical service however as soon as externally provided services are introduced the Service Catalog becomes a vital planning and operational function. Planning to ensure new cloud services will integrate with current

services and once they are implemented operational contractual conditions are being met. One important item performed by Service Catalog Management is to ensure there is no unofficial usage of cloud services because this could incur extra costs and possibly other contractual penalties.

Services provided by external cloud computing still need to perform the important basic activities such as such as service level agreements (SLA)s because they define important levels of service such as availability and performance. Services processed by the cloud still need SLAs and the associated IT-customer relationships that drive their creation. It is the role of service level managers to communicate with IT customers and create appropriate SLAs with their input. In the case of services that are provided externally (e.g. outsourcing or cloud services), SLAs are built to ensure contractual commitments are translated into working processes. This is to ensure they can be measured and analyzed, especially if penalties are invoked for missing SLA targets. Service level agreements, together with underpinning contracts, provide the basis for the concept of a warranty for a service or a system. It is for these reasons that service level management is so critical for users of external cloud computing.

Service design questions

AVAILABILITY MANAGEMENT

- Is there an agreement between IT and the cloud suppliers specifying when and how planned outages should be scheduled?
  - > *Failure to specify and agree on potential times for scheduled outages or method to agree scheduled outages could mean downtime or delays for essential changes.*
- Are there agreed availability timings and usages with the potential cloud computing users?
  - > *The impact of not answering this question depends upon the contract agreed upon with the cloud suppliers, because if there are cheaper charges for off-peak usage then the potential cloud users should understand and agree to these charges to avoid potential financial penalties.*

CAPACITY MANAGEMENT

- Have current and future volumes been calculated and used to determine current and future capacity requirements for service and applications that will be submitted to cloud computing?
  - > *If contracts are negotiated against potential usage levels then it is imperative that accurate capacity calculations are performed failure to do so could mean paying higher rates for cloud services. The best prepared party in a contract negotiation situation usually gets the best deal.*
- Is the capacity being monitored on an ongoing basis and as a result are trends being identified?
  - > *Changes in capacity or capacity growth can mean that improved contracts can be negotiated without measuring and calculating capacity it is more likely that financial penalties will be invoked rather than improved contracts negotiated.*

IT SERVICE CONTINUITY MANAGEMENT

- Do potential external cloud suppliers have disaster recovery plans?
  - > *Many cloud suppliers claim that due to the design of the cloud it is very unlikely that a disaster will happen. This may be true, but if the supplier does not have a disaster recovery plan then the risk is obvious and repercussions could be devastating.*
- Is constant research being performed to identify cloud failures elsewhere? And if they are discovered, are they checking with current cloud suppliers to ensure that they have protection in place?
  - > *When utilizing the cloud the "it will not happen here" syndrome is not acceptable because of the implications. Therefore it is necessary to constantly monitor the web for examples of failure and obtain assurances, or proof, that protection is in place.*

INFORMATION SECURITY MANAGEMENT

- Have the levels for service management security been checked and agreed upon? For example, the security for managing the lifecycle of a change?
  - > *Failure to establish security levels for components such as change and asset management could provide a backdoor entry for potential criminals.*
- Have regular checks been planned to check the security quality provided by the external cloud computing suppliers?
  - > *Checks need to be performed to ensure that service management is resilient to security breaches. Failure to do so will mean that security violations will not be located, allowing criminals extended access.*

SUPPLIER MANAGEMENT

- Have cloud contracts with suppliers been checked by international lawyers?
  - > *What is a legal contract in one country may not be legally binding in another country; as the cloud suppliers could reside in other countries, it is important that contracts be verified to ensure that complications do not arise at a later date (e.g. ownership of data).*
- Are there tools in place to check that suppliers are meeting their contractual obligations?
  - > *There are many reasons why external cloud computing may be adopted. But to maximize the benefits for these reasons it is vital that cloud suppliers meet their contractual commitments—which is why tools need to be in place to make the necessary checks.*

SERVICE CATALOG MANAGEMENT

- Do you check your Service Catalog regularly to ensure that your customers are only using the services to which they are entitled?
  - > *Unofficial usage of cloud services could incur extra costs and possibly other contractual penalties which is why constant vigilance is essential.*
- As a planning function do you plot all potential new cloud services into your Service Catalog to highlight potential clashes and other potential operational issues?
  - > *Failure to plan how new cloud services will fit in with other services is essential otherwise there could be performance, availability, capacity and change problems that would be avoided with a well maintained Service Catalog being used as part of the cloud planning activity.*

SERVICE LEVEL MANAGEMENT

- Are service level agreements, operational level agreements, and underpinning contracts defined, documented, and agreed upon for the governance cloud services?
  - > *SLAs, OLAs, and UCs are essential to contract negotiations and as a benchmark to govern the services provided by cloud suppliers. Without them customer expectations will not be satisfied.*
- Are there activities to monitor, measure, report, and review the level of IT services provided by cloud computing in place?
  - > *It should be possible to monitor, measure, report, and review the level of IT services for all of the components described in the SLAs, OLAs, and UCs. Failure to do so could result in customers receiving poor service for longer than necessary.*

Summary

The importance of service design cannot be underestimated because the next stage is to take the design and turn it into a deliverable service. Beware of haste and underestimating the complexity of cloud computing. These are the enemies. This stage in the lifecycle should not be circumvented in any way because the better the foundation, the stronger the result.

How does service transition work with cloud computing?

Service transition is the IT twilight zone that exists as services or applications progress from a development environment into live processing. Like the twilight zone, service transition can be full of pitfalls that await the unprepared. Unfortunately, many of these pitfalls occur as a result of a loose attitude toward transitional planning that has arisen as a result of internally supported applications and services. The pitfalls can be easily and quickly resolved for internally supported systems, but externally supplied technologies, such as cloud services, can be much more unforgiving. For example, if you have planned and contracted a service for 100,000 transactions a week with an external cloud supplier and that limit is exceeded, then expansive penalties could apply or service degradation could be incurred. This is why, in the case of externally supplied cloud services, it is vital that transitional planning is performed diligently. Externally supported cloud computing is vulnerable because the more external factors involved in a change or transition, the more difficult it becomes to resolve issues, especially if the external cloud service is to integrate into locally resident technology. A quick glance at the service transition processes illustrates their importance to successful implementation of new services and to the upgrading of current services, including: change management, service asset and configuration management, release and deployment management, service validation and testing, transition planning and support, evaluation and knowledge management.

The most obvious and most important component of service transition is change management, because failure to manage changes will result in lost time and resources for IT customers. Change is difficult when all of the components for a change are in-house. This difficulty grows exponentially when there are external factors involved, especially if those components are based in a nebulous cloud environment. It is not just the possibility for failure that is a factor; e.g., who does the external cloud supplier notify when a change is to be implemented, who will explain any new functions to the users, and how do external cloud users request a change? For any change to be a success all parties involved in the change or affected by the change need to be involved in the change process, and at the very least get change schedule notifications. A failed unauthorized change performed by the cloud supplier could have dire circumstances. One other factor is making certain that security rules are not broken during a change allowing a miscreant to perform criminal activities.

Service asset and configuration management are interesting components when employing cloud services. For example, if all services were supplied from cloud computing sources then the only assets would be peripheral devices—such as smart phones, laptops, and printers—and configuration management would scarcely exist, but we are a long away from this scenario at the present time. Configuration management has a critical role to play when it comes to cloud computing, because it has to identify the relationships between the local traceable configuration items (CI) and the remote cloud components, and then integrate them into configuration management. This is no easy feat. The better the local configuration is managed and the CIs relationships are properly maintained, the smoother the changes and upgrades will be

performed. The individual cloud suppliers will need to have their own CIs in the configuration management data base (CMDB) so they can be absorbed into the local CMDB for planning, change, and risk assessments purposes.

One of the greatest advantages of release and deployment management is that new software releases utilize the attributes of cloud computing. Release management is simplified because once a new release has been deployed on the web, all of the users of that software will automatically use the new release as soon as they load or refresh the software. The problem is ensuring that clear notification is given to all those users logging on to the new software. This example also illustrates how cloud-resident software removes many of the barriers associated with deployment and roll-outs. There is the problem of ensuring the releases issued by the cloud supplier will be compatible with other software that is in place. It is possible to foresee a day when a new end device, Smartphone, or laptop will be issued with very little resident software—making deployment even easier, with the bonus that users will be able to configure their own devices with only the services and applications they need. (E.g., a user may use only Microsoft Office Word and Excel, so why would that user load PowerPoint and Outlook?) The days of a standard corporate footprint are numbered; it is more likely there will be a number of standard footprints for the plethora of remote devices now available to the end IT customers (e.g., one footprint for a iPhone and another for a Blackberry).

One area that will continue to alter with the advent of cloud computing is service validation and testing, because validation and testing focuses on the operational aspects of a cloud application, rather than on the programming. With external cloud services the level of customization is often limited, meaning that service validation and testing must concentrate on selecting the external cloud service supplier that best matches the needs of the client, rather than build a bespoke system for them. Of course services will still need to be validated and tested to ensure they function correctly and they provide the services required by the users. It is just that more diligence will need to be applied when validating and testing the services provided by the external cloud suppliers. For example, ensuring the external cloud supplier meets all of the conditions in the service portfolio before signing any contracts (whereas often internal systems are implemented with known errors that are corrected after implementation).

One of the forgotten components of ITIL is the evaluation process, described in the service transition book as “the actual performance of a change… assessed against its predicted performance and any deviations between the two… understood and managed.” In a nutshell, making sure changes meet expectations. With locally-based systems, it is important that changes meet expectations. When those changes occur in a remote or virtual environment controlled externally checking that the change delivered meets its expectations is essential partially because of the potential fallout and partially to ensure the change does not have negative effects. It must be remembered, with external cloud computing, IT no longer controls the change process but is instead a participant in the process. IT needs to perform their role in the change process, including evaluating the predicted outcome of a change against the actual outcome of a change.

The final process of service transition is knowledge management, which is expected to ensure the right information is delivered to the appropriate place or competent person at the right time to enable informed decision making. In the early days of IT most of the programs and services were written and implemented internally. This made it easy to control and manage the knowledge required by IT to support those services because the knowledge was internal. But this changed as soon as purchased solutions and outsourcing became more prevalent. As we progress on to cloud computing it becomes a case of the more services supplied externally, the less knowledge there is to maintain. More importantly, it becomes harder to maintain that knowledge because local knowledge no longer exists to enable successful decision making. We now live in a world where it is not what you know, but whether you can locate the knowledge you require; it is not just a case of storing knowledge, but being able to quickly identify and locate that knowledge. In the case of cloud computing it is imperative that cloud suppliers provide online knowledge to their customers to support the services they supply.

Service transition questions

CHANGE MANAGEMENT

- As an organization, have you ensured that you are integrated into the change management process used by your cloud suppliers? Are you kept fully in touch with the status of all changes that may affect your cloud services? Did you have a chance to provide input concerning planned cloud changes?
  - > *The consequences of not being informed and involved in potential changes can be catastrophic, especially if any changes implemented by the cloud supplier fail or affect performance. Changes have always been the Achilles heel of IT, but with the advent of cloud computing and the subsequent reduction of control over changes IT must adopt a customer role in change management, ensuring any changes performed are necessary and will be implemented successfully. It is important to have the technology resources to track and manage changes by cloud suppliers and the ability to integrate the management of those changes with other non-cloud changes so a comprehensive view of changes can be observed and of course managed.*
- Does the cloud computing contract include any compensation for failed changes such as financial penalties or other forms of compensation?
  - > *The cost of failed cloud computing resources can be very expensive. For example, what if an organization only lost their email service for a day? How would that affect normal business routines and what would be the resulting cost? There will be resistance to compensation and financial penalties from the cloud supplier, but without such assurances cloud computing may not be as attractive for high business-impact services. Again, technology needs to be in place to be able to track failed changes and their associated costs.*

SERVICE ASSET AND CONFIGURATION MANAGEMENT

- Can the configuration for assets be visualized to include resident technologies and cloud technologies plus any integration between them to provide one view of the configuration for a given service?
  - > *Handing over management of a service to a cloud computing supplier does not mean handing over asset and configuration management. The difference is the cloud service will become part of overall configuration management. It is important for risk and decision management that cloud services be viewed in context with the rest of the components required to provide an overall business service. Failure to manage the inclusion of cloud technologies into the overall configuration could result in poor risk analysis and subsequent poor decision making. Technology that can provide visualization needs to be in place. In the case of a CMDB, all cloud IT services should be included as CIs so their relationships can be traced and identified. Remember governance still needs to be applied.*
- Is there a relationship with the external cloud supplier to ensure that all devices required to interface and integrate with the external cloud service meet the current and future requirements of the cloud service? For example, is it possible to determine which of the current smart phones in use can cope with an update to a cloud computing service?
  - > *With cloud computing, one of the biggest challenges is ensuring the devices connected to the cloud meet the current and future needs of the cloud services. Not only can all of these devices be tracked, but they also have the capabilities to meet future needs of upgrades to the cloud service. The impact of not being able to provide this service could delay new releases of cloud services or result in major down-time for the Cloud service users.*

RELEASE AND DEPLOYMENT MANAGEMENT

- Is there a single location where the release, version, and license data of all software and media required to support and use cloud services are kept?
  - > *It is essential that all locally maintained cloud related software (e.g., relevant versions of web navigation software) is kept in the in-house definitive media library so that it is accurate and easy to locate. All updates to versions or releases must go through change management so that the definitive media library (DML) remains an accurate and reliable source of data. Failure to maintain this information could result in failure to meet some governance requirements, but will result in flawed planning for updates and upgrades. For example, a change may require that all smart phones have version X of a software component installed but many of these devices still have version Y—which will cause the change to fail when implemented, causing downtime for customers. It is essential cloud suppliers provide accurate and timely notification to ensure that the integrity of the DML is maintained to the highest possible levels (e.g., prior notification if a new release of a web browser can be utilized).*

- Can the configuration of all cloud computing related technology be viewed in context to the service?
  - > *Change, problem, incident, and event management can be delayed by issues when locating the correct versions of releases, versions of cloud-related software, and media—which is why a key component of deployment is the planning required to ensure smooth and trouble-free deployment of new and updated technologies. This planning can be hastened by having the accurate DML data available in a configured format so relationships between the components can be viewed and assessed for deployment. Although the DML contains all of the data describing cloud-related technologies, this needs to be federated with the CMDB so that deployment planning can be performed with confidence. Cloud suppliers must take an active role in deployment of their technologies, supplying data and other services to IT so that deployment plans are accurate and feasible. Release and deployment has always been a cocktail of IT, technology suppliers, and business managers, but it now has the extra ingredient of cloud suppliers who must be included in release and deployment where applicable.*

SERVICE VALIDATION AND TESTING

- Are all cloud services carefully validated to make sure that they meet the service design and therefore meet the customer's requirements?
  - > *One of the features of cloud computing services is their lack of customization—meaning that often customers have to tailor their working processes to meet the functionality of the cloud service. This means that services must be validated with the customers before allowing new cloud services or systems to be implemented. Users of cloud computing services may require more training to make the adjustment from the current physical and virtual working practices to the new cloud-supported working practices (e.g., using a smart phone is a lot different to using a work station). Service design or specification should include the essential business requirements and associated functionality for any proposed cloud service so that training and documentation can be prepared. Failure to do so will result in delayed implementation and failure to fully utilize the power of cloud computing.*
- Have the proposed cloud services been tested in a fully integrated environment?
  - > *Cloud services are designed to rigid standards that include the specification needed by any supporting technologies, e.g. which web browsers and which version of those web browsers can be used. Therefore it is essential to test the integration of those supporting technologies to ensure smooth deployment.*

EVALUATION

- Are cloud services assessed to determine their acceptability?
  - *ITIL quotes evaluation as "a generic process that considers whether the performance of something is acceptable, value for money etc." This quote obviously applies to all services but has specific pertinence to cloud services because these would have been justified on cost and performance and therefore need to be evaluated to ensure that they deliver on any claims made concerning lower costs and improved performance.*
- Are cloud services regularly measured or reviewed to ensure that they continue to meet their specifications?
  - *It is quite possible that a cloud service will meet its obligations when it is implemented, but will it continue to meet those obligations as time progresses? Cloud services must be regularly reviewed because factors such as demand will change and the cloud supplier must be able to support this trend. This applies to all services, but in the case of cloud suppliers scalability can become expensive; if an organization is tied into a specific contract, then handling extra levels of capacity or performance can prove to be punitive.*

KNOWLEDGE MANAGEMENT

- Are all facets of external cloud computing documented and readily available to IT technicians and support staff?
  - *The more remote a service is from IT the less knowledge is available on site for technicians and support staff. Therefore it is essential the cloud supplier provide excellent and easily accessible remote knowledge. This should be tested during service validation and testing. The existence of remote knowledge should not reduce the effort and commitment to produce and manage local knowledge.*
- Are there measures in place to stay abreast of any issues that may apply to a cloud service?
  - *Vigilance is essential when dealing with external suppliers especially if they are cloud-based and difficult to contact compared with traditional services. It is a good idea to utilize social media groups to exchange information concerning cloud computing services.*

Summary

Service transition can be described as a point of no return because it is often very difficult to reverse a faulty new service once it has been implemented. This is why so many small fixes are applied immediately after implementation. One point to keep in mind is that once a service is implemented, the organization utilizing the cloud becomes responsible for the legal implications for that service (for example, ensuring that it meets Sarbanes-Oxley specifications). Therefore every aspect of service transition should check that governance is being adhered to. There is one interesting aspect here—if the Cloud supplier resides in another country and is not meeting Sarbanes-Oxley specifications, is this an offense? And if so who is the guilty party—the organization using the cloud or the cloud supplier?

How does service operation work with cloud computing?

Service operation is a key component of ITIL because it is where the rubber meets the road. Extending IT into the cloud is no different— it's still all about providing service delivery and keeping true to IT's customer commitments. If an IT department's deployed service strategy is correct, the design appropriate, and the transition successful, its service delivery should meet or exceed expectations regardless of deployment methodology. But adopting a cloud-based strategy will require that many established operational service tasks be performed remotely. When planning on adopting a cloud strategy, or any new technology for that matter, it all comes down to having good processes and functions in place.

For example, which service desk should a user of a cloud service contact for support—the in-house service desk or the cloud supplier's service desk? It's a simple enough question but the answer can have major ramifications. If the cloud service desk is to be used, care must be taken to insure support contracts deliver adequate levels of support. Additionally, if the cloud service desk is selected to perform traditional in-house support the resulting shift may impact the in-house service desk's headcount as a result of offloading responsibilities. When applied across the roles performed by service operations—service desk, incident management, problem management, request fulfillment, access management, event management, technical management, IT operations management, and applications management—it becomes very clear why process transition is so critical to get right. And don't forget, delivered services remain in operation long after the design and transition phases are complete, so any cloud transition strategy needs to be resilient as well as efficient.

The service desk is an interesting place to start when planning a cloud transition because, for most organizations, this is a well-established resource whose basic principle of being a single point of contact is now under threat. In cloud-based deployment models most of the technology required to support a business service resides outside of IT and so too does the knowledge required to support that service. For example how do you answer typical "how do you do X" questions when the user knows more than the service desk? First of all, readily available accurate knowledge relating to the cloud service is essential so users can access knowledge on demand rather initiate a service desk contact. If a user fails to find a solution in the knowledge resources the next step would be to contact the service desk. At this point there are basically two choices: the user contacts the resident in-house desk who treat the cloud service desk as second level support, or allow the users to contact the cloud desk as a first point of contact. The role of the service desk is vital for cloud computing, which means that the performance of knowledge resources and the cloud service desk need to be carefully and constantly monitored for performance and observed for quality of service.

The service desk typically is where incident management is performed—tracking and managing incidents throughout the incident lifecycle. So determining where this responsibility resides is key to understanding how the support process is defined prior to moving to the cloud. Once the most effective first point of

contact for the service desk has been decided, in-house or at the cloud, it is extremely important to realize that, for a successful implementation, the responsibility of managing incidents still resides with the originating company through an established IT service management process. If the service desk is cloud-based, then it is essential that a detailed list of all cloud-based incidents logged are supplied on a regular basis to customers' ITSM process so that they can be analyzed for continual service improvement. Ideally users should log and send their incidents electronically so data provided by the cloud suppliers can be cross-referenced with incidents logged by users. Ideally both the cloud service supplier and their customers should access the same incident management tool, allowing for incident/problem process transparency and thus, complete synergy between users and the cloud supplier.

The key to problem management is in finding the root cause of an incident, or series of incidents, and to take appropriate actions to eliminate the root cause. Normally this is straightforward process but it becomes more complicated when the root cause may lie within the services provided by a cloud supplier. Since cloud suppliers will want to apply their own priorities and timing for eliminating root causes to their services it is important the roles concerning problem management are clearly specified in any contracts or agreements. Having all affected parties on the same support tool will simplify reporting, service level management, as well as the tracking/and management of outstanding problems.

Customers and users must have a source where they can make requests of IT with a high likelihood of fulfillment. As described by ITIL, request fulfillment is "*a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists"* (service operation). Since cloud suppliers will play a key role in the request fulfillment lifecycle having strict bounds on what can be requested of them is critical. Insuring cloud engagements success requires that "pre-defined approval and qualification process" exists. Having these processes in place greatly improves the likelihood that a cloud supplier will be capable of performing any requests submitted to them. Just as important as it is to create request fulfillment processes, it is also equally important they be referenced in any contract or agreement with cloud suppliers to protect both parties.

Access management is concerned with granting authorized users access to a service along with the rights to which functions of a service they can utilize (rights and identity management) or in other words managing access security. This is a constant challenge for in-house shops but this is exacerbated dramatically when a third-party supplier enters the arena and is one of the greatest challenges concerning cloud computing, i.e. just how secure is the cloud service?. Although the cloud supplier could be responsible for managing access it is the responsibility of the in-house service to manage both rights and identify management. To provide an extra blanket of security it is prudent to involve customer management in the planning and vigilance of access management. All access must be carefully monitored and assessed by the purchasing company's ITSM organization and/or security authorities. Since the implications of a cloud service security breach could prove catastrophic to a customer's organization the application of a strong governance approach can prove beneficial; obtaining ISO/IEC 27000-series or similar international certification can be reassuring in verifying necessary steps are taken to secure cloud access management.

One of the prime roles of event management concerns taking corrective action when alerts occur; for example, an alert may be issued as a warning that capacity is getting dangerously close to being exceeded. Once this alert is recognized and registered appropriate action can be taken to restore the capacity balance. Sensible alerts are the backbone of a well-built service, but just how does a cloud supplier respond to them without the proper authority? In the preceding example of responding to a capacity situation would the cloud supplier have the authority to increase capacity, even in the increase would involve generating extra revenue for that capacity? The secret to successful event management using cloud computing is to identify all possible alerts and their corrective actions with each cloud supplier, and pre-define the appropriate actions they would be allowed to institute to resolve and remove alerts. Failure to do this could result in delays resolving alerts, reducing customer service levels, or possibly incurring unplanned costs by allowing cloud suppliers to take unauthorized actions.

Technical management plays a vital role because it ensures that all resources required for infrastructure support are trained and deployed to design, build, transition, operate, and improve infrastructure technology. It should be very clear that technical management must be included in all of phases selecting and employing a cloud supplier. Failure to fully involve this resource could delay cloud service implementation and increase costs due to inadequate infrastructure planning. Technical management is charged with ensuring that the resources required to support the infrastructure are in place, but IT operations management is responsible for performing the day-to-day activities, operational tasks, functions, and processes.

IT operations management is as old as IT itself but is often overlooked, which could prove disastrous in the case of cloud computing. Unless regular day-to-day activities are performed at the correct time serious faults can occur to disrupt customer services. IT operations management specifications must clearly state who will perform operations actions and contain the work instructions explaining how to perform those actions.

To quote ITIL, "applications management is to applications what technical management is to the IT infrastructure" and, as such, the same comments apply here as they did for technical management—except they should be applied to applications.

Service operations questions

SERVICE DESK

- Are there clearly established prime contact points for users of cloud computing services?
  - > *It doesn't matter which manner of technology is employed, but a single point of contact for each customer and user has proven itself an essential tool for high-quality customer and user support. With cloud computing, another layer of technology is being introduced that will require integration with the existing customer support system and processes. Customers must know who to contact for support and how to communicate with that contact point (e.g. telephone, email, Web, or direct access to a specialized support tool). Failure to establish a prime contact point will frustrate and delay support to cloud service customers.*

- Are the relationships and responsibilities between the service desk and cloud support documented, contracted, and understood?
  - > *Failure to include service desk roles and responsibilities attributed to cloud computing suppliers for cloud support will result in extra costs and excessive down time for customers. Remember, cloud suppliers are required to meet their contractual requirements and will charge for any services provided outside their contractual boundaries.*

INCIDENT MANAGEMENT

- Are the tools and roles in place for accurate incident logging?
  - > *Accurate logging of incidents has always been a source of information, knowledge, and data for ITSM to reduce the number of future incidents, manage the incident performance lifecycle, and provide a valuable resource for continual service Improvement process. Since incidents are very likely to occur in the cloud it is essential these incidents are trapped and logged so preventative action can be taken. There must be agreement between customers and their cloud suppliers to determine incident management roles and responsibilities. Even if the same support tool isn't used to record and log incidents, links should be established between the cloud supplier's system and the customers ITSM system. Having a closed loop incident reporting process is key to preventing future problems and maintaining transparency with the cloud supplier.*
- Has the lifecycle ownership of incidents been established and contracted?
  - > *Trapping and logging incidents is only the first step in a process—the lifecycle ownership of incidents needs to be established and agreed upon. Without lifecycle ownership incidents can remain unresolved, causing excess workload for the service desk due to repeated incidents not being resolved by the cloud suppliers along with associated SLA breaches. Incident lifecycle ownership must be established with cloud suppliers and be considered an important part of the contract.*

PROBLEM MANAGEMENT

- Is there a mechanism in place to allocate the responsibility for eliminating a problem or known error?
  - > *The first step in handling problems is to identify a work-around so that the users can continue uninterrupted, the second step is locating the root cause and then identifying persons capable of eliminating the root cause. On some occasions workarounds will not exist, which will mean the only course of action is to find the root and eliminate it. For in-house support services allocation of responsibilities is an easy task, but cloud suppliers will need to be treated as second level support, requiring them to undertake the same responsibilities expected from typical tier 2 level support groups.*

- Is there a process in place for a joint workforce to be established for critical problems?
  - > *This situation occurs when a service cannot be restored to users within the agreed upon service levels without the root cause being identified and eliminated. Just identifying a root cause can be a challenge, therefore it is important that a joint workforce with representatives from the customer and cloud supplier be initiated as soon as possible to jointly locate and eliminate problems. Interrupted services need to be resolved fast without time being wasted trying to decide who will look for the root cause. Therefore this needs to be addressed upfront in contractual agreements.*

REQUEST FULFILLMENT

- Have standard request fulfillments been agreed to and documented, including who is responsible for which requests? I.e. is a request the responsibility of in-house services or the cloud service supplier?
  - > *It is quite likely that a cloud supplier would be responsible for fulfilling a request. Therefore it is important to quantify and agree upon these standard requests with the cloud suppliers so that they understand their request fulfillment responsibilities. It is possible that the suppliers will charge for these requests. If this is the case then all requests should pass through in-house service fulfillment to ensure that costs and service are being carefully managed.*
- Do both parties have access to common technologies to identify customer requests?
  - > *It is important to keep track of all proposed requests to ensure that they are fulfilled. Cloud service suppliers must have access or integration with the customer's request system to efficiently accept, track, and fulfill requests. Standardized access will ensure availability of a central repository to manage request fulfillment. Not having a central technology resource could result in overcharging, missed requests, or requests that have been fulfilled twice.*

ACCESS MANAGEMENT

- Have the authorization levels and responsibilities been documented and contracted?
  - > *Every time an external source is added to the IT infrastructure potential for security breaches increases. Therefore it is critical that every effort be made to ensure all parties clearly understand their levels of authority and associated responsibilities. Merely understanding authorization levels and responsibilities is not sufficient and should be documented in contractual agreements; cutting corners when dealing with access management is not acceptable.*
- Checking for breaches—what actions are to be taken if a security breach is suspected?
  - > *The key to successful access management is constant vigilance and fast reactions if a security breach is suspected. Continuously monitoring for security breaches requires sophisticated access management software to identify potential breaches and key to staying secure. Of equal importance are the actions to be taken if a breach is suspected since the longer a breach is allowed the more damage that can be inflicted. Technology should be employed to identify breaches and fully documented action plans must be created, understood and practiced. This applies to both the cloud supplier and internal customer security services.*

EVENT MANAGEMENT

- Are there appropriate alerts in place to support the cloud computing service?
  - > *Documented contractual commitments are the key source for identifying appropriate service alert levels. For example, if a contract has documented the requirement to support 10,000 transactions per day then it may be wise to set an alert at 9000 transactions so appropriate action can be undertaken if required. Alert objectives should set to ensure that customers receive agreed levels of service as specified in the contract. It is the responsibility of in-house ITSM to ensure these alerts are in place; failure to put them at the right levels will result in extra costs and the inability to deliver agreed upon service levels.*
- Are the technology and processes in place to recognize, register, and initiate appropriate actions when required?
  - > *If the correct alerts are in place then there must be appropriate technologies and processes in place to recognize and register when an alert is raised and initiate the appropriate actions. This may require specialized software but its use must be considered to guard against potential losses due to missed alerts, e.g. extra costs for too many transactions or reduced performance due to capacity warnings being missed. Managing alerts is an ongoing activity because new alerts will always need to be added as technology requirements change, as cloud contractual agreements change and as missed alerts are identified.*

TECHNICAL MANAGEMENT

- Is technical management involved in all phases of planning with the cloud supplier?
  - > *Technical management is important to cloud service success—it is responsible for the design and building of local infrastructure necessary to interface with the cloud infrastructure. This cannot be achieved successfully unless technical management is involved in all phases of cloud supplier selection.*
- Do the technical management and the cloud supplier communicate regularly with each other concerning infrastructure?
  - > *Many problems can occur if technical management and cloud technical management are not in perfect harmony. To ensure both infrastructures are tightly integrated local technical management and cloud technical management should communicate regularly to ensure that no anomalies arise, and that the infrastructures are prepared in time to meet the requirements of any planned changes.*

IT OPERATIONS MANAGEMENT

- Have the operational activities that relate to cloud computing been given clear operational responsibilities?
  - > *The more platforms resident in an organization the more operational activities are likely to be performed. Therefore when a new platform or technology such as cloud computing is added to the mix it is very important to allocate ownership, especially if the actions are to be performed by the cloud supplier. This applies even in a single platform IT shop because, with the introduction of cloud computing, it is likely that anew platform will exist with a different set of parameters.*
- Does IT operational management have clear instructions for all operational activities related to cloud computing?
  - > *Whether the operational activities are to be performed locally or remotely they must be created and clearly documented. Depending on the activity, failure to do so could mean deployment delays or other operational risks.*

APPLICATIONS MANAGEMENT

- Is applications management involved in all phases of application planning with the cloud supplier?
  - > *Even though a service may be provided by a cloud supplier it is still comprised of one or more applications. Therefore applications management is still important to cloud computing. Successfully building services or interfacing with the cloud infrastructure requires the involvement of applications management in all phases. In many cases cloud applications will require integration with the local application; e.g., a cloud application and a local application may share the same database.*
- Do applications managers and cloud supplier need to communicate regularly with each other concerning the resilience and functionality of cloud based applications?
  - > *Lack of applications functionality can occur if applications management and cloud applications management don't work together. To ensure applications meet a customer's requirements, the customer's applications management and cloud applications management teams should communicate regularly.*

Summary

Service operation is primarily concerned with the actions required to support a "live" service that is in full production and an integral part of the services supplied by IT to the business. Irrespective of the strategy, the design and accuracy of transition for most of the lifecycle of an application is in the hands of service operation. No matter how well engineered, a mistake by service operations can cause a crash just like a car—it doesn't matter how sophisticated the design, for most of the life of a car it will be in the hands of a human and is sooner or later bound to get damaged. This is why this often-neglected back-office IT activity is extremely import for the success of cloud computing. The skills and knowledge accumulated and managed by the service desk are essential to supporting cloud computing because very little service knowledge will reside elsewhere in IT. Equally important is the data in the incident management database, which when analyzed will identify any areas where cloud suppliers are not meeting their contractual agreements. If incident management does indentify weaknesses then problem management needs to work with the cloud supplier to ensure the supplier identifies the root cause and eliminates the problem as soon as possible. Request fulfillment becomes more complicated if many of the requests are to be fulfilled by an external resource such as cloud computing. Ensuring that requests are fulfilled and their progress monitored is an essential task performed by service operations.

Another key role for service operation is access management, which controls and manages access rights and identity management so the risk of illegal access to cloud resident data is minimized. Poor access management can have a catastrophic effect on an organization. Constant liaison between cloud suppliers, technical, and applications management is important as they need to work together to implement new applications and technical software updates, which means that service operations become the customer representatives in this process.

When you collate all of the activities performed by service operation you could describe the service as the warranty management center, because a large part of the service operation role is to ensure that cloud computing services meet their contractual deadlines. Another key consideration is the knowledge that service operation collates as it performs it regular duties. Why is this so important? Because all of the applications software and much of the technical software utilized by cloud computing are sourced from an external resource, which means there is a knowledge vacuum to be filled by service operation.

Service operation is not the most glamorous function in IT but, because it has daily contact with both cloud suppliers and cloud customers, it has a unique role in providing and supporting cloud computing. It is essential that service operation is included from the very outset at the Strategy phase and through the complete implementation lifecycle so that it can be integrated with the services provided by the cloud suppliers.

About the author

Recently Malcolm was a member of the ITIL Advisory Group (IAG) who were responsible for overseeing the development and publishing of ITIL v3 plus he was a mentor for the Service Transition book. In 2009 Malcolm was awarded the coveted Ron Muns Lifetime Achievement Award for his work in the IT Service Management arena.

Malcolm Fry, is a recognized IT industry luminary with over 40 years experience in Information Technology. Malcolm is the author of many bestselling books on IT Service Management, and has had numerous articles and papers published. He is regularly used as a source of information by technology journalists. He is also the solo performer in a highly successful best selling DVD series made for the Help Desk Institute explaining the relationship between the ITIL processes and the Service Desk. He has written 6 ITIL focus booklets of which over 100,000 copies are now in circulation. His previous publications include 'A step-by-step Guide to Building a CMDB' and 'How to build and ITIL Service Management Department' while his latest publication 'ITIL Lite' is due to be available early 2010.

Malcolm began his IT career in 1967 working for a major bank in London. In the following 13 years he performed many IT functions including system programming and a variety of management roles. During the same period, Malcolm worked in a number of industries including retail, production, oil and pharmaceuticals. This experience, coupled with his impressive technical background, gives Malcolm an unparalleled breadth of knowledge and experience.

Malcolm began his independent career in 1980 and since that time Malcolm has not only pursued a solo career, but has also been on the boards of various organizations, including Protocol International Limited and Help Desk Institute's Strategic Advisory Board. He was on the ITIL Advisory Group helping to guide the development of ITIL v3 and was a mentor for one of the books. During his long and diverse career, Malcolm has worked in more than forty countries, lectured to countless people and is in constant demand worldwide as a dynamic, entertaining and knowledgeable speaker.

Malcolm has devised the 'Front of the Front Office' theory, which explains how technology can be used to create new marketplaces and products for enlightened organizations. As a result, he is often asked to present at conferences his views on how technology will affect both business and our everyday lives. These sessions are steeped in reality, without resorting to complex technical theory, and do not fly into the realms of fantasy. His views on futures are widely respected and he advises organizations on how to maximize their business return on technology by looking for new business opportunities. He is both innovative and informative and has the unique ability to communicate his thoughts with audiences who have regularly voted him best speaker on many conferences worldwide. He is also sought after as a strategic consultant by many large organizations worldwide. Most of these organizations use Malcolm as a catalyst to review their facilities and processes from which he assists them to determine their requirements, and most importantly, prepare plans which allow them to meet their objectives from within.

CS0105_1010