Service Management and Cloud Computing

This is the third in a series of six postings looking at the impact of the new realm of service provision on the traditional way of managing services as per the ITIL framework.

The postings cover:

1. Agile Methodology
2. DevOps and CI/CD
3. **Cloud Computing**
4. Digital Transformation
5. Lean Thinking
6. Internet of Things (IoT)

A brief explanation of Cloud Computing (As I understand it!)

One huge component of any IT service provider is **Infrastructure Management**. Some aspects involved are Architecture and Design, Purchase and Installation, Capacity Management, Patching, Network Management, Security, Licencing, Decommissioning, the list goes on. (See ITIL manual of the same name for an idea of all this discipline involves).

Since these disciplines are common to all Datacentres, it should not be surprising that such work has become commoditised. Organisations specialise in this work and profit due to economy of scale and vast resource sharing. These organisations provide Cloud Computing.

When deciding to adopt Cloud Computing, an enterprise is agreeing to outsourcing their IT Infrastructure Management – removing the ownership and risk of managing in-house. **THIS IS CRITICAL** to realise and understand! It means how the infrastructure is provided and maintained is not the concern of the cloud service recipient.

Think about it. Trying telling a plumber HOW to do their job, and see how far you get.

Infrastructure is provided as a Service (IaaS). The recipient enterprise Requests infrastructure from their cloud provider, and it becomes available within minutes, or even automatically (scaling out) provided the right conditions are met.

Many of the management headaches are gone. Or at least they have morphed into other headaches. Sorry, I mean, other considerations to manage.

NB: With advanced cloud providers, their offerings will also include Platform as a Service (PaaS) and Software as a Service (SaaS). These are additional layers to the infrastructure which are commonly in use. Consider what suits when designing the architecture of your service.

There are a few different models of Cloud, each with their pros and cons.

1. Private, where the entire cloud is owned and used by one enterprise (either on or off premises).
2. Public, where the enterprise chooses to make use of a Cloud available to any organisation (although securely segregated) or
3. Hybrid, which is combination of the other two cloud models.

What does this mean to Service Management?

The biggest thing Service Management providers need to understand is that Cloud Computing is providing Infrastructure as a SERVICE. There must be a clear **demarcation** between the service being provided, which the enterprise needs to be manage, and the infrastructure underpinning the service, that the enterprise does NOT need to manage.

In moving to Cloud Computing, an enterprise must first prepare for the move – have the ability to let go of some Service Management functions and disciplines.

The Infrastructure Management in a Cloud is a service. The recipient of this service must manage infrastructure based of SLAs and Service Requests.

Activities within the Cloud, such as upgrading, patching, backups, failovers, are **not** the responsibility of the recipient, and accordingly, they have no right to be involved in the infrastructure at an Event, Incident, Problem or Change Management level.

These ITIL disciplines must still exist in the recipient enterprise, but only for services NOT in the cloud, or where the infrastructure service has issues. **Change Management** is only involved where there are major works involved in moving processing to the Cloud.

The Cloud Provider owns and manages the infrastructure. The Cloud Services Recipient manages the Data and Processing (software) that runs in the Cloud. This is reflected in the **AWS Shared Responsibility Model of Cloud Security**.

Too many Cloud Computing endevours fail because the Recipient does not understand, or is not really prepared, for this new paradigm in their IT world.

Infrastructure must become a **Service Request** from the Recipient's **Service Catalogue**, controlled by the requestors' access. The Infrastructure Service must have its full conditions of service clearly spelt out in the SLA covering the Cloud Provision.

Incident Management is not the failure of any infrastructure in the Cloud, instead it must relate to when the Cloud Service does not meet the SLAs.

Configuration Management must record Cloud Infrastructure as a Service, **not** as hardware. Recording instead, which systems or applications use these services. The Configuration Items within the Cloud must remain a black box to the Recipient enterprise.

Change Management, as far as Cloud Computing is involved, is restricted to the verification and approval of moving processing to the Cloud.

Security Management becomes the specification, and verification, of the security levels that the Cloud Provider must comply with. Most recognised Cloud Providers will exceed the security needs of those enterprises where Technology is not their core business.

Capacity, Availability and **Service Continuity Management** are major planning exercises when designing or enhancing the enterprise services. They will lead to further specifications of what must be provided by the Cloud. The challenge for these disciplines then becomes the verification of such capability.

Of course, Cloud Computing does not come free. **Financial Management** must be capable of tracking Cloud Recourse usage of an hourly (and with some providers, minute based) use. What are the rules for who can request what of the Cloud? How will this be controlled?

Ensure your cloud provider is able to provide accurate data on usage, and this data is auditable.

Like with all major changes in the technology realm, business must first decide and document **why** they want to go down the cloud computing path. What benefits does business expect to achieve by moving to Cloud Computing, and how will these benefits be verified?

Setting these goals out clearly will also help understand the impact on Service Management. The benefits become Key Performance Indicators (KPIs). Variations from the 'norm' must be quickly detected and addressed. Service Management has a new game to play.