WHAT DOES IT SERVICE MANAGEMENT LOOK LIKE IN THE CLOUD?

An ITIL based approach

Marc Jansen
Computer Science Institute
University of Applied Sciences Ruhr West
Tannenstr. 43, 46240 Bottrop
Germany
marc.jansen@hs-ruhrwest.de http://www.hs-ruhrwest.de

Abstract: - In recent years a new approach for the dynamic usage of computational power, memory and other resources comes into play: the Cloud Computing paradigm. This new approach needs to be concerned with respect to IT Service Management since cloud based infrastructures have to be managed differently from a usual infrastructure. This paper discusses, based on the IT Infrastructure Library (ITIL), as the de-facto standard for IT Service Management, what kind of processes needs to be concerned especially if a certain service should be deployed in the cloud.

Key-Words: IT Infrastructure Library, ITIL, Cloud Computing

1 Introduction

In recent years a new approach for the dynamic usage of computational power, memory and other resources comes into play: the Cloud Computing paradigm. The term "Cloud Computing" was first used very frequently without an exact definition of what Cloud Computing actually is. This changed as the National Institute of Standards and Technology (NIST) presented a definition of the term Cloud Computing [1]. This new approach provides a paradigm that allows to dynamically provide computational resources, e.g. computational power, memory, … and is therefore especially interesting for IT Service Providers. Since cloud based infrastructures have to be managed differently in comparison to usual IT infrastructures, a closer look towards a practical approach of IT Service Management with respect to Cloud Computing is necessary.
On the other hand, IT Service Management is a topic of interest for quite a while already and the IT Infrastructure Library (ITIL), as its de-facto standard, is already available in version 3. Nevertheless, this version does not yet deal with the specialities that need to be concerned with respect to Cloud Computing.
Therefore, this paper discusses on the basis of ITIL which processes needs to be concerned especially for the topic of Cloud Computing.
After a short explanation of Cloud Computing specific terms and a short introduction into the ITIL theory, a discussion of certain ITIL processes and their importance with respect to Cloud Computing are presented.

1.1 Short Introduction to Cloud Computing

Cloud Computing implements a completely new approach towards the provision of computational services that provides both advantages and challenges to IT Service Management. Basically some of the processes that have been very important in a service provision without the usage of Cloud Computing become less important in cloud based scenarios. Vice-versa other processes become more important by making use of cloud services.
Usually Cloud Computing is separated in three different categories [2]:

1. IaaS - Infrastructure as a Service: Virtual provision of computing power and/or memory. A prominent example of an IaaS service is the Amazon WS service.

ISBN: 978-1-61804-030-5

2. PaaS – Platform as a Service: Provision of a runtime environment, like application servers, databases, … In this area, Googles App Engine is probably the most prominent example.
3. SaaS – Software as a Service: Provision of usually browser based applications that can directly be used. Here, Google Docs or the Customer Relationship Management software of salesforce.com might serve as examples.

Another categorization that is used within the area of Cloud Computing describes the question whether a publicly available cloud is used (public Cloud Computing) or a privately owned cloud, e.g. by one company, is used (private Cloud Computing). Also a mixture of these two types, so-called hybrid clouds, is possible. The question whether to use a public, a private or a hybrid cloud is especially interesting with respect to security issues. For example a company might be willing to put a certain service into the cloud, e.g. to gain more flexibility within the service provisioning, but might be concerned about security aspects if the data, the service operates on, is no longer into direct reach of the company, e.g. in its own datacentre.

1.2 The IT-Infrastructure Library: a short Overview

The IT Infrastructure Library (ITIL) provides the de-facto standard for IT Service Management processes. It is currently available in version 3. According to the current version of ITIL a service runs through several lifecycle phases during his life, as shown in Figure 1:

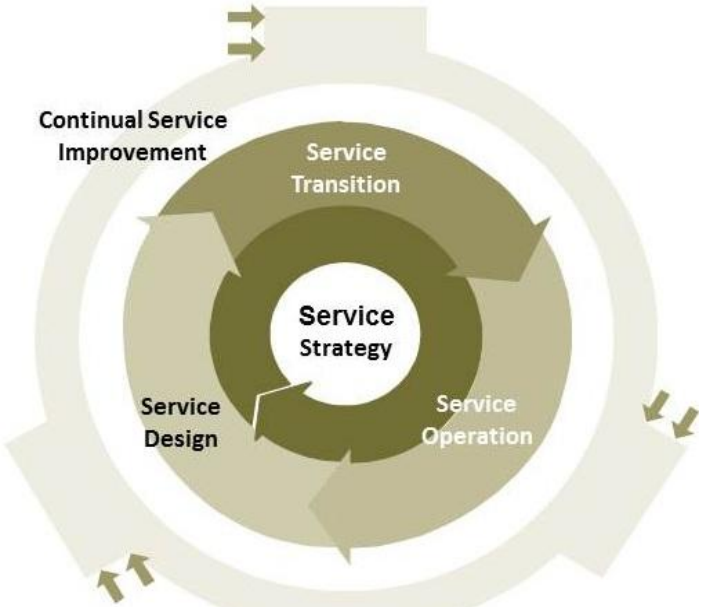

Figure 1[1]: The ITIL lifecycle approach

Within the Service Strategy lifecycle phase, strategic decisions towards a service are made, e.g. which service should be provided for which customer or what kind of new services a company will provide.
The second lifecycle phase, Service Design, is responsible for designing new services or to design changes in existing services to increase their quality.
The necessary processes to transport services from the Service Design phase to operation are provided by the Service Transition phase, e.g. necessary processes to ensure that new or updated services are set into operation in a controlled way.
Within the Service Operation phase the services are running and produce an added value for the customers. This lifecycle phase provides e.g. processes like Incident Management or a process for the handling of Service

[1] © Crown Copyright 2007 (OGC).

Requests. Last but not least, there is a special Lifecycle phase for the continuous improvement of services that is responsible to increase the efficiency of the services provided. Table 1 shows which lifecycle is primarily responsible for which processes.

Table 1: ITIL lifecycle phases and according processes

Lifecycle Phase	Processes
Service Strategy	Service Strategy Process, Service Portfolio Management, Demand Management, Financial Management
Service Design	Service Level Management, Service Catalog Management, Availability Management, Information Security Management, Supplier Management, Capacity Management, IT Service Continuity Management
Service Transition	Change Management, Service Asset and Configuration Management, Release and Deployment Management, Knowledge Management, Transition Planning and Support, Service Validation and Testing, Evaluation
Service Operation	Incident Management, Problem Management, Event Management, Request Fullfillment, Access Management
Continual Service Improvement	7 Step Improvement Process, Service Reporting, Service Measuring

As the name “library” already indicates, each of the five lifecycle phases is published in one book.

2 Discussion of the ITIL lifecycle phases with respect to Cloud Computing issues

The following provides a discussion about the certain ITIL lifecycle phases (and their corresponding processes) that have special aspects with regard to Cloud Computing. All processes that does not need to be considered especially in Cloud Computing environments, are not discussed.

2.1 Service Strategy

From a strategic point of view [3] within the Service Strategy Process it has to be identified what kind of services are candidates to be deployed in the cloud. Usually not all services can be run in the cloud, e.g. due to security restrictions. Especially if the service is a candidate to be deployed in a public cloud, the customer needs to accept that the data, on which the service operates, is no longer in direct reach of his own datacentre. That is usually no longer an issue for already outsourced services. Nevertheless, when it comes to business critical services one or the other customer might still think critical about this issue.

Furthermore the Demand Management process is a critical one for deploying a service in the cloud since this is the process that describes the performance needs of a certain service from a business perspective. In order to later on, in the design phase, allow the cloud provider to provide the necessary capacity for the service (within the Capacity Management process) the cloud provider needs to understand the capacity demands of the service from a business perspective. This is the only way to allow the service provider to really fit the capacity needs of the customer.

Last but not least, the Financial Management process needs to provide the necessary data in order to decide whether a certain service can be deployed more efficiently in the cloud [4]. The Financial Management process also has to deal with a major problem of cloud based scenarios: the customer is usually very much interested in knowing the costs for a certain service before he runs the service. In a cloud based scenario where the cost is usually calculated at a per usage base, the cost for certain services can not be calculated a priori. This might be an advantage for one or the other service, but might as well be a problem for one or the other customer. Therefore, the Financial Management process needs to provide solutions for the a priori calculation (or at least an upper boundary of the costs) and the flexibility of the costs in a cloud based scenario.

ISBN: 978-1-61804-030-5

2.2 Service Design

For the design [5] of a new or changed service in a Cloud Computing scenario the Service Level Management process is extremely important. Since a huge amount of the responsibility is transferred towards the Cloud Computing provider, the Service Level Agreements (SLAs) need to reflect that. Therefore, especially the relevance of the underpinning contracts (UCs), that are in the responsibility of the Supplier Management process, need to be considered.

Another critical aspect is the availability and the capacity of a service that runs in a Cloud Computing scenario. Of course the availability of the service, as well as the performance of the service needs to be as described by the business demands with the Demand Management process. Therefore, depending on the choosen Cloud Computing scenario (IaaS, PaaS, SaaS) both, the availability and the capacity provided for the service need to be guaranteed. It is of high importance that the SLAs are negotiated at a reasonable level: in an IaaS scenario it does not make sense to negotiate an SLA with respect to response time of a certain service, but it would make sense to have a guaranteed amount of memory in the probably virtual environment. On the other hand if the service is provided by a SaaS scenario, the arrangement of an SLA based on the response time would make perfect sense. Here we find a close relationship between processes like the Service Level Management, the Availability and the Capacity Management in conjunction with the Supplier Management process.

Another important process, with respect to Cloud Computing, of the Service Design lifecycle is the Information Security Management process: As already said before, it needs to be accepted (at least in a public cloud scenario) that the data on which my service operates is no longer available in my direct reach, e.g. in my privately owned datacentre. Therefore it needs to be checked from a security perspective if it is possible to put the data for the services in question in a public datacentre. Again, this is not so critical for service that are already outsourced, but it may be critical for services that are newly created or updated. Furthermore other boundary conditions need to be concerned, e.g. within the European Community it is not allowed to store private data of individuals outside the European Union [6]. Additionally, a security concept within a cloud based environment needs to be set up completely different than in a usual environment. Well-known security mechanisms like perimeter firewalls, demilitarized zones and intrusion detection systems do not work in cloud based environments. This is basically due to the high level of virtualization on which cloud based infrastructures are usually build. Moreover traditional aspects like the hardening and minimal installation of the operating system, user and rights management and user data encryption become more and more important within cloud based environments. For example a service provider that provides IaaS scenarios might want to provide extremely minimalistic machine images, on which only necessary services are deployed, PaaS and SaaS providers might concentrate more on encryption of both user and communication data.

Additionally within the Supplier Management process the need for a deeper understanding of the related software licenses is necessary. Some software companies might prohibit the use of their software in virtualized environments. On the other hand software licenses based on a “per CPU” bases do not scale very well in Cloud Computing scenarios. In the cloud, software licenses that are more related to the amount in which a certain software is used, scale a lot better, e.g. software licenses per user or (nowadays quite unusual) the amount of time a certain software is used.

One major advantage of moving a certain service into the cloud is that the IT Service Continuity Management process is no longer of high interest since the Cloud Computing provider guarantees a certain availability, also with respect to disaster recovery.

2.3 Service Transition

Within the lifecycle phase Service Transition [7] the results from the design phase are brought into production. Therefore especially processes like the Change Management process and the Release and Deployment Management process are important for this phase.

One of the major goals of the Change Management process is to decrease the number of incidents due to changes and to provide mechanisms that allow to deploy changes in a controlled way. Within a cloud based environment the Change Management process needs to consider other services when deploying a change to one

service. Since most of the commonly available IaaS scenarios are based on virtualization, potentially a large number of other services might be influenced by the work necessary to deploy a change to a single service.
On the other hand, the major goal of the Release and Deployment Management process is the protection of the productive environment. This process becomes even more complex since the complexity of a cloud based infrastructure is usually higher than the complexity of a non-cloud based infrastructure.
But also the service transition phase can benefit from deploying a service in the cloud: the usually very complex Service Asset and Configuration Management System becomes a lot easier. The major goal of the Service Asset and Configuration Management process is to provide an overview about all the parts (so called assets) of the infrastructure and the interrelations that are necessary to provide a certain service. This process is outsourced to the cloud service provider since he is responsible to run his infrastructure. Here, again the oursourcing level is highly dependent on the cloud scenario (IaaS, PaaS or SaaS) in question. In an SaaS scenario the cloud service provider will be responsible for the complete Service Asset and Configuration Management process whereas in e.g. an IaaS scenario the cloud service provider will only be responsible for the infrastructure part of the Service Asset and Configuration Management process. The customer itself is in an IaaS scenario only responsible to provide the configuration management information about the used platform and the relationship between the used applications.

2.4 Service Operation

The Service Operation [8] lifecycle phase it the phase where the services are provided to the customers and where the added value for the customers is generated.
Processes like the Incident, Problem and Event Management do not run completely different in a cloud based environment in comparison to a not cloud based environment. Anyway, at least in a public cloud scenario some cloud based services are outsourced. Therefore, a high integration for the Incident, Problem and Event Management process of the cloud service provider and the corresponding processes at the customer site is necessary. Furthermore, the Access Management process becomes more important in cloud based scenarios. As already stated, usual security mechanisms like a perimeter firewall, demilitarized zones and intrusion detection do not work very well in cloud based environments. Therefore, the only way to protect the data is to provide a reasonable concept for the access rights of the data and the resources provided in the cloud.
Additionally, the Request Fullfillment process, that is responsible for the fulfilment of small user requests, e.g. resetting a password, becomes more powerful from a user perspective. Usually standardized changes can often be applied over the Request Fullfillment process. Within ITIL a standardized change is defined by low costs, low risk and the change has to be run successfully at least once before. If all these criteria are met, a certain change can be made a so-called standard change and these kind of changes can usually later on be applied over the Request Fullfillment process. In a cloud based scenario all these criteria are met also for increasing a certain resource, like computing power or amount of memory. Changes at this level are now able to be deployed over the Request Fullfillment process which is completely not possible in a not cloud based scenario. Therefore, it could be said that the Request Fullfillment process becomes more powerful in cloud based scenarios.

2.5 Continual Service Improvement

The Continual Service Improvement [9] phase is responsible to ensure that the provided services are provided more efficiently over time. This is the major goal of the 7 Step Improvement Process. With respect to cloud based scenarios the quality improvement might be to put as many service as reasonably possible in a cloud based scenario to increase the flexibility of the service and, at the same time, to decrease the cost of the services in question. Therefore, this process should concentrate on the delegation of good experiences in the cloud to other services. Additionally, to allow for the measurement of service quality, the Service Measuring process is also in the responsibility of the Continual Service Improvement lifecycle phase. This process becomes more and more important in cloud based scenarios, since it is responsible to provide key performance indicators that can on the one hand be used in the Service Reporting process and on the other hand in the 7 Step Improvement Process to determine possible potential of services and especially cloud based services.

ISBN: 978-1-61804-030-5

Last but not least, the Service Reporting process is responsible for the reporting of service quality and to provide the data that allows to proof that a certain service level was reached or not. As already said, the negotiation of Service Level Agreements (SLAs) is extremely helpful in cloud based scenarios and therefore a mechanism that allows to control these SLAs becomes more and more necessary as well.

3 Summary and Outlook

The discussion shows that ITIL, as the de-facto standard for modern IT Service Management, can also be applied for the IT Service Management of Cloud Computing environments. Yet, most of the processes need to be considered differently in comparison to a usual, not cloud based, infrastructure.

From a customer point of view, the lifecycle phases for the strategic decisions and the design of certain services will be more complex if the service should later-on be deployed in a cloud based environment. Thus, the later lifecycle phases like the transition and the operation phase, are more likely to be easier to handle, at least if a public cloud of an external service provider is used. This is mainly due to the fact that the responsibility for these lifecycle phases is in this scenario outsourced to the service provider in question. Within the phase of continual service improvement, both, the customer and the service provider, need to work hand in hand to improve the quality of the service.

From a service providers point of view, the first two lifecycle phases are not of high importance. A service provider here only has to provide interesting attractions in order to motivate a customer to put at least some of his services into the cloud. The other way round, the lifecycle phases of the transition and operation of services are more important from a service provider point of view, since these are the phases where he produces the added value for his customers.

Moreover, the discussion shows that ITIL in his current version has not yet set up specialized services with respect to Cloud Computing. This might probably be the case for the upcoming version of ITIL, but since Cloud Computing is already quite interesting for a large number of customers, and the number of service providers in the area of Cloud Computing is constantly growing, there is actually already today a need for IT Service Management in the cloud. ITIL provides a good basis for this, but needs to be considered differently at least in some processes.

Acknowledgements

This work was partly supported by an Amazon AWS research grant.

References

1. Mell, P., Grance, T., 2009. The NIST definition of Cloud Computing. Version 15
2. Chappell, D., 2008. A short introduction to cloud platforms: An enterprise oriented view. San Francisco, CA: Chappell and Associates.
3. Igbal, M., Nieves, M., 2007. Service Strategy: Office of Government Commerce (ITIL). The Stationary Office Ltd.
4. Reese, G., 2009. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O'Reilly
5. Rudd, C., 2007. Service Design: Office of Government Commerce (ITIL). The Stationary Office Ltd
6. European Community, 1995. Directive 95/46/EC. Official Journal L 281.
7. Lacy, S., 2007. Service Transition (ITIL). The Stationary Office Ltd
8. Cannon, D., 2007. Service Operation: Office of Government Commerce (ITIL). The Stationary Office Ltd
9. Spalding, G., 2007. Continual Service Improvement: Office of Government Commerce (ITIL). The Stationary Office Ltd