Service Management In A Cloudy World

White Paper

Charlie Miles
Management Consultant
Pink Elephant

Executive Summary: Service Management In A Cloudy World

As the use of cloud services continues to increase in most organizations, IT Management is generally managing how best to utilize cloud services but they are struggling with how best to transition from a technology-centric organization to a service-centric organization, and figuring out what their own role within the organization will be in the future.

Most organizations have incorporated cloud services as part of their portfolio, but the use and reliance on cloud services is accelerating at a rapid pace. The challenges these organizations are faced with will therefore need to be addressed and managed more closely, and this is where Service Management becomes more critical.

This white paper presents some trends and challenges facing many organizations, and some basic guidance to become more strategic and tactical in your Service Management approach in order to better address, manage and utilize cloud services as part of your overall portfolio. In doing so, this will help you solidify the role of your IT department within your organization in the cloudy world of the future.

Cloud Services; A Brief Introduction

The adoption of cloud services has been increasing steadily for several years. Not so long ago, many organizations were struggling with the decision to enter the world of cloud services, though ironically many of these same organizations had been using Application Service Providers (ASPs) for many years. There were many reasons why they were struggling with this decision, not the least of which was security and regulatory concerns and costs. However, as IT organizations increasingly face having to provide more services with fewer resources, and as the challenges of cloud services became easier to manage, the usage of cloud services continues to increase.

Definitions

Before some baseline statistics are presented to illustrate the growth of cloud services, some definitions are provided for clarification as many of these terms are used interchangeably, or – as is often the case – the term 'cloud' is simply used to cover all of these.

Application Service Provider (ASP): Companies who provide access to their software via the internet. While there are several differences, the main difference between an ASP service and a cloud service is that ASPs do not provide the infrastructure to their clients; they simply provide the application and access to the application.

Public Cloud: IT resources, such as applications and storage are available to the general public, either free or on a pay-per-usage model. Public clouds share infrastructure with multiple businesses. However, these shared environments aren't suitable for all businesses as the public cloud may not be appropriate for mission-critical workloads, security and regulatory requirements and concerns, availability requirements or management demands.

Private Cloud: Similar to the public cloud, but delivered through a proprietary architecture and dedicated to a single organization which offers more scalability, self-service, multi-tenancy, on-demand changes, etc. This service is suited for businesses that have dynamic and unpredictable computing needs that require more direct control. Private cloud can be hosted outside of your firewall, but also can be offered on-premises which require additional management, staffing and maintenance overhead.

Hybrid Cloud: A mixed use of public and private cloud.

Software as a Service (SaaS): Considered a type or category of cloud service; a software distribution model in which a supplier hosts the application and offers subscriptions to access and use the applications. This eliminates the need for on-premises infrastructure, hardware and software.

Platform as a Service (PaaS): Considered a type or category of cloud service; a service that delivers applications over the internet, along with the hardware and software tools needed for application development. While the provider hosts the hardware, software and infrastructure, the user-businesses have the option to host their own hardware and software and the ability to perform their own development functions.

Infrastructure as a Service (IaaS): Considered a type or category of cloud service; a service that provides virtualized services over the internet. The provider hosts the hardware, software, servers, storage and other components on behalf of its user-businesses. This is typically used for very dynamic, temporary, developmental workloads that change frequently, and is also used for automation of administrative tasks, dynamic scaling, desktop virtualization and policy-based services.

The differences between ASP and cloud services; between public, private and hybrid clouds; and between SaaS, PaaS, and IaaS are critical for IT Management when making strategic decisions regarding the use of cloud services. Note that this white paper is not about cloud services themselves, so the very brief descriptions are provided simply as reference.

Statistics

There is a multitude of data available from many sources regarding the use, adoption and growth of cloud services. This white paper specifically references one source that is publicly available; *Right Scale - Cloud Computing Trends: 2016 State of the Cloud Survey; published February, 2016.*

Readers can dissect the numbers presented here and dispute the source, that's OK. This white paper is not about the numbers and, indeed, the actual statistics and metrics will differ slightly based on the source. The point is to illustrate some key elements about the direction, adoption and use of cloud services, now and in the future.

Right Scale surveyed 1,060 IT organizations. Ninety-five percent of these organizations are currently using cloud services:

- 18% use only public cloud services
- 6% use only private cloud services
- 71% use hybrid cloud services

On average, these organizations:

- Use 1.5 public clouds and 1.7 private clouds
- Are expecting to expand an additional 1.5 public clouds (total of 3) and 1.3 private clouds (total of 3) in 2016
- 17% of surveyed enterprises now have more than 1,000 virtual machines in public cloud – 13% growth over 2015
- 31% of surveyed enterprises are running more than 1,000 virtual machines in private cloud – 22% growth over 2015

But what's more interesting, and is the real focus of this white paper, are the challenges that are faced by the surveyed organizations in utilizing cloud services:

- Lack of resources/expertise (32% of organizations)
- Supplanting security (29%)
- Compliance (26%)
- Managing multiple cloud providers (26%)
- Managing costs (26%)
- Complexity of building a private cloud (24%)
- Governance and Control (23%)

- Performance (15%)

Early, in the history of cloud services they were viewed as being low-cost alternatives to providing services in-house, however this did not prove to be reality. As the survey shows, managing the costs of cloud services is a real challenge. In response to this, the surveyed organizations are looking to *optimize these costs*:

- Monitor utilization and right-size the solutions
- Automate shutdown of temporary workloads
- Shutdown workloads during certain hours
- Look for storage volumes not in active use
- Select cloud or region based on cost
- Move workloads to cheaper cloud/region
- Utilize public clouds (such as Amazon, Azure and Google) where possible

However, each of these cost optimization options need to be weighed against the risk of doing so. One last significant statistic from the Right Scale survey is the adoption of DevOps. DevOps, along with cloud services are two critical enablers to deliver software applications faster. This survey shows that DevOps is adopted (or being adopted) by 74% of surveyed organizations, up from 66% the previous year.

What this survey and the statistics presented illustrate is that:

1. Cloud services are no longer considered optional, the only thing that is optional is which types of cloud service to utilize, for what strategic purpose
2. Service Management is now more important than ever

Service Management

Service Management, as most everyone knows, is defined as "…a set of organizational capabilities for providing value to customers in the form of services." The organizational capabilities include your human, technical, and capital resources as well as the skills, knowledge and expertise.

A common misconception often heard when organizations were deciding to move into the world of cloud services was that they did not need Service Management, or more specifically, the framework that we so lovingly refer to as ITIL[®]. This misconception was based on the assumption that Service Management and ITIL were intrinsically linked to the technology but in fact Service Management isn't really about the technology; it has always been about using technology appropriately to provide value through services. By definition, Service Management makes no distinction as to where the technology resides or who manages it.

Service Management is more critical now precisely because there is less direct control over the technology, yet you are still accountable for delivering value through the effective management of the services and, by extension, the various service providers.

Value Chain-Shift In Focus

The question more often asked now is how Service Management applies in a world where we are depending less on on-premise technology and more on external service providers. To answer this you need to look at the provisioning of services as a value-chain; plan-build-run. You still need to plan it, you still need to build it, and you still need to run it. What changes in this scenario are the people and organizations involved as part of the value-chain; instead of or in addition to your own technical resources you will rely more on external resources to build and run the service. But you are ultimately still accountable for the entire value-chain.

Most IT organizations perform at the operational level and the transition to operations well or at least well enough – this is the run piece of the value-chain. Yet, there is still a struggle with the strategic and tactical elements and the transition from development, this is the plan and build parts of the value-chain. While the operational – or run elements – will still be necessary to some degree, the critical focus now needs to be on the strategic and tactical – or the plan and build. So it is a matter of shift in focus, not just from technical to service but also from operational to strategic and tactical.

Operational/Technology

Let's talk about the most obvious first, the technical and operational elements of Service Management. No, technology will not go away completely. Even if you utilize cloud services for all of your applications, platforms, infrastructure, and even if you utilize desktop virtualization you still need to monitor, manage, and support the end-points and the traffic from your firewall to and from those end-points. You still need to manage the access to these services from within your organization, you will still have requests related to the services as well as for consumables that your cloud providers probably won't provide, and you still need to provide a level of customer support and service for your business customers. Imagine making your customers determine which provider they need to call based on an incident or request with a specific service; this is a potential nightmare for your business customers and you can't allow that to happen.

Operational support may take on a different form and structure than what it is currently within your organization, but the need for this does not go away. While this is important, it is equally important to focus on the strategic and tactical elements of Service Management in order to provide true value to your business through cloud services, whether all or just a portion of your services are provided through the cloud.

This is where a lot of organizations that are technology/operational-centric in their approach sometimes struggle, but this is also where all IT organizations need to excel in order to survive and succeed in the cloudy future.

Strategic

Earlier, the challenges that organizations face in utilizing cloud services were listed; lack of resources and capabilities, security, compliance, managing multiple cloud providers, managing costs, the complexity of building a private cloud, and governance and control. Addressing these challenges and making the right business decisions around these challenges is, in part, strategy. The decision to utilize cloud services is not, or should not be made on a whim, or as isolated point-solutions – though this does happen quite a bit, especially where business units are allowed to engage cloud services outside of IT's awareness or control. Careful thought and strategic planning need to go into this at two levels.

The first level is your approach to incorporating cloud services as part of your overall service portfolio and service strategy. This is an overarching strategy that must consider business risks, security and regulatory concerns, as well as cost implications (not necessarily cost reductions). For those organizations who charge back for services, you must also determine how the costs of cloud services are rolled up into your charge-back model.

The second level is strategy related to specific services and changes to those services. At this level, you need to consider which portion of the service, if any at all, is best provided by cloud services, and what type of cloud service is necessary; whether or not it can be satisfied by lower-cost public cloud or requires a private or hybrid cloud approach.

I also listed earlier some specific methods that organizations are employing to optimize costs; monitor utilization and right-size the solutions, automate shutdown of temporary workloads, shutdown workloads during certain hours, look for storage volumes not in active use, select cloud or region based on cost, move workloads to cheaper cloud/regions, and utilize public clouds where possible. All of this necessitates a sound risk management approach and an excellent understanding of your business demand and capacity, but you must also have a firm understanding of the business requirements for the service and whether or not those requirements can be met by a public cloud service offering or requires the flexibility and control provided by a more costly private or hybrid cloud service.

Basically, this is service strategy '101'; a solid foundation of service strategy management, service financial management, service portfolio management, service demand management and business relationship management. Without a solid understanding and foundation of service strategy, you cannot ensure that you have a proper or consistent approach to cloud services as part of that strategy. The decision to utilize cloud services is not and cannot be a series of isolated solution-point decisions.

Tactical/Design

With a solid strategy in hand, it is now time to apply that strategy to the planning and building of your services, whether this be an initial deployment of a service or is an update or change to an existing service. At this point it is often tempting to select a vendor and hand it all off to them. There are many variables that go into the proper selection of a vendor and negotiating a win-win contract, including the availability and capacity requirements and flexibility of those requirements, the necessary security controls and service continuity requirements, and the commitments you want or need to make with your business as to levels of service and support provided. More complex services or services that are more specific or inflexible with requirements typically result in a private or hybrid cloud and high-cost contracts.

But even before you consider the vendor and the contract, in order to determine the requirements and levels of service that are necessary and acceptable, you have to ensure all design elements are in place. The Service Design Package, or SDP, which includes everything about a service that is critical for the operation and support of the service, needs to be addressed and included. Much of this starts with your organization and will be added to by the vendor as they build and deploy the service, and certainly the more vanilla the service the easier this is; but you still need this and this is still your

responsibility. This is the only way to know with any certainty whether a vanilla public cloud offering is sufficient or if you need a more complex and costly private or hybrid cloud approach, and how the latter needs to be designed and delivered.

Now consider the level of complexity, when you need to integrate multiple services from multiple vendors, where you need to share data, transfer files, and connect the integration points and ensure support provided by each vendor that is involved. A viable goal is to reduce the total number of vendors that you engage for all of your services as this reduces overall risk and can work to reduce costs, but more than likely you will still have multiple vendors. This requires a general-contractor approach; whether or not you do this for yourself or engage in complex managed services, you are still accountable for this, and it is part of the overall design.

Tactical/Transition

Your vendors will have the primary control over the technical elements of your cloud service, the changes they make to their own infrastructure and applications and the changes they make based on your enhancement requests will have direct impact on your business. These changes cannot be made without prior knowledge, awareness and preparation within your organization. In order to ensure this, and in order to ensure that you have the proper level of participation and control over these changes entering your environment is a matter of contract and vendor relationship management, both which are discussed shortly.

However, from a release and change perspective – you are the customer. And as such, you need to have review and sign-off capability of all service design plans and you need to be able to perform testing and have sign-off capability on the test results and the ability to stop or delay a change as a result. And while you may have little control over the actual deployment schedule, the change should never be a surprise to you.You need to always be prepared which includes ample time for communication and training for those impacted by the change. The recording, management and authorization of the change and the management of the release and deployment cycle need to take place within your Service Management control. Again, it does not matter who has hands on the technology, these are your services.

Further, the vendor should provide you knowledge and known errors, or at least access to knowledge and known errors related to the service and changes to the service – just as if you were building, testing and deploying the technology yourself. This information should be provided to you and you need to manage it within your knowledge and problem management systems prior to deployment; as well as provide or coordinate any necessary training to operations and to the users of the service.

Vendor Management

Your level of involvement in the control, design, testing, deployment and support of cloud services depends directly on the terms and conditions of the contracts you agree to with your service providers. Over the years, I have worked with clients who are unhappy with their vendor contract/service/relationship and want to achieve better service from their vendors. But when I looked into the contract and their issues, what is typically found is that the organization is much to blame for this; not necessarily the vendors. The cause of poor contracts typically starts with poor requirements, or lack thereof, and/or poor integration with existing contracts and vendors which often is caused by lack of a common strategic approach. Further, once they have agreed to and signed the contract they have to live with those terms and conditions. Often the culprit is the desire to cut costs and therefore entering into the lowest cost contract. The phrase "you get what you pay for" takes on a whole new meaning when it involves putting your organization at risk through a poorly aligned service contract. With increasing use of cloud services for critical business functions, the greater the risk imposed on your organization.

A challenge I noted earlier that organizations are faced with in utilizing cloud services is performance; both the performance of the service in terms of service levels as well as performance of the vendor in delivering the service within the agreed terms and conditions. Another issue typically seen is that after a contract is agreed, the vendor and the relationship is not adequately managed and minor performance and relationship issues can fester and become a conflict necessitating costly conflict management, early termination of the contract, or worse yet, the failure of the relationship that imposes severe risk on the organization; all because resources were not available to, or were not managing the performance of the vendor or the relationship with the vendor appropriately.

In the world of cloud services (or anything that involves an external vendor), everything ultimately boils down to one thing, and one thing only; adherence to the terms and conditions of the contracts. You get exactly what you agreed to, and what you paid for. Nothing less, nothing more. It is therefore absolutely critical that if one wants to achieve success in providing value through cloud services, one must become expert at vendor management; there is no other choice.

Conclusion: The Quadrumvirate For Success In A Cloudy World

Several Service Management topics have been covered in the short space of this white paper and one of the main messages is to apply more focus on the strategic and tactical elements of managing your services, but don't lose focus on the operational element.

There are four key areas, or the quadrumvirate, for success in ensuring value to your business through the use of cloud services as part of your overall Service Management strategy. These areas are:

- A holistic strategic approach for the use of cloud services as part of your portfolio, and the appropriate application of that strategy individually and specifically for each service
- A solid understanding of business requirements specific for each service to determine the best use of cloud services; focus on value and not purely the cost of the service
- A holistic, strategic and tactical approach to managing vendors, beginning with the engagement of vendors for contract negotiation and extending through the lifecycle management of the performance of the service and vendors, and the ongoing relationship with the vendors
- An explicit yet flexible change management and release and deployment management process and control of all changes that vendors make to cloud services as they impact and affect your business

While you may not need the same level or amount of technical skills and resources in your environment as things get cloudier, you will most definitely need to transition towards a high level of strategic and tactical Service Management skills and the right resources to bring this cloudy world into focus.

About Pink Elephant

We Lead The Way!

A premier global training, consulting and conference service provider, Pink Elephant has an undisputed reputation for leading the way. We're proud of our pioneering and innovative spirit, which has enabled us to introduce and spearhead many revolutionary concepts and programs since our inception forty years ago.

About The Author

Charlie Miles is a certified ITIL Expert with many years of practical experience in the IT industry as a Service Management practitioner, manager, consultant, and trainer.

Contact Us

www.pinkelephant.com

1-888-273-PINK

info@pinkelephant.com