Whitepaper

Managing the Public Cloud: Who Owns What?

Introduction

When it comes to management responsibilities of a cloud environment, confusion still reigns at many organizations about the complexities involved. A lot of IT and business executives do not have a clear sense of their various roles and responsibilities, including what they should be doing and what can be left to the cloud providers to handle.

There is also uncertainly about the skill sets required for migrating data and native workloads from on-premises systems or private clouds to the public cloud, and day-to-day management responsibilities even after a cloud migration is complete.

In many cases, IT leaders assume that public cloud service providers own all of the management responsibility. There's a "set it and forget it" mentality that perhaps comes from a perception that companies are outsourcing their IT responsibilities to a service provider.

That perception results in a big mistake, and it can lead to cost overruns, security weaknesses, systems downtime, and other issues. The problem is, determining management responsibilities in a cloud environment can be more complex than many might think. The reason for that is the responsibility for particular tasks and processes varies depending on the type of cloud service being provided.

For example, customer responsibilities will be different for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings. With so many organizations beginning to move to a cloud strategy that encompasses one or more of these types of cloud services, it's easy to see how things can evolve into a state of confusion.

It's important to note that regardless of the type of cloud service, IT operations management still exists within the cloud; it's just different. There's fundamentally a need for new skill sets, new processes, and new tools.

This whitepaper looks at how the roles and responsibilities differ depending on the type of cloud service, and provides guidance as to what organizations should be doing when it comes to management of IT as part of a move to the public cloud.

Getting past the confusion

Before we examine each of the main types of public cloud services, it's important to look at what's happening out there in the world of cloud services — and where things are going wrong from a management perspective.

Based on industry research, there's apparently a broad misconception in the market about who is responsible for what when it comes to the public cloud. For example, a **2017 report** by research firm Vanson Bourne and data management provider Veritas showed that more than two-thirds (69%) of 1,200 global business and IT decision makers wrongfully think their organization's cloud service provider covers all data privacy, regulatory compliance, and data protection. This dangerous misconception could result in a company being fined large amounts of money due to possible loss, mishandling, and/or compromise of their core business data.

The research shows that when it comes to public clouds specifically, there are likely misconceptions about which party holds the ultimate responsibility for data management: clients or the cloud services provider.

A majority of the organizations surveyed that use or plan to use IaaS offerings (83%) expect their organization's cloud providers to protect their workloads and data against outages, and more than half (54%) think it's the responsibility of the service provider to securely transfer data between on-premises and the cloud. About half of the organizations think the cloud service provider is responsible for backing up workloads in the cloud.

These are just some examples that document the cloud management problem. But the findings make the point that there is clearly a disconnect as to the level of responsibility for management of cloud services. IT leaders and their business executive counterparts need to take ownership of this issue and work to clear up any misunderstandings that might exist with their cloud providers before problems get out of hand.

Determining whether there is a problem with cloud management responsibilities and acknowledging this problem needs to be the first step for organizations. After that, resolving the issues of cloud management will basically require having the right people, processes, and tools in place.

It's important for organizations to understand that management responsibilities can vary considerably depending on the type of cloud service. The following sections outline internal IT team responsibilities when deploying different types of public cloud services.

Client responsibilities with IaaS

With IaaS, a service provider delivers virtualized computing resources to customers via the internet. The cloud provider hosts IT infrastructure components that were typically part of the traditional data center, including servers, storage systems, and networking equipment, in addition to the virtualization technology.

IaaS offerings might also include a variety of services such as security, storage backup, systems monitoring, billing, load balancing, clustering, and optional failover.

Many organizations are adopting IaaS offerings from public cloud service providers as they look to move away from premises-based servers and storage systems. The common drivers are cost savings and increased agility.

In an IaaS engagement, the physical layer of the IT infrastructure goes away for the customer. But from an operating systems perspective, setting and configurations are still the responsibility of the customer, as are the management of applications and data.

The enterprise client is responsible for monitoring and patching all the operating systems in place to make sure they continue to comply with governance and client hardening standards.

Depending on the IaaS service being used, the client might also be responsible for:

Data protection

Disaster recovery

Data governance

All of these are significant responsibilities. If operating systems are not kept up to date and configured correctly, data and applications are not managed adequately, data is not protected effectively, and disaster recovery and data governance strategies are not in place, the entire endeavor will likely collapse, and the business impact could be severe.

When creating contracts with IaaS providers, all of the possible management issues and responsibilities need to be worked out in detail prior to cloud service delivery. That will help prevent any misunderstandings about who is responsible for what.

Client responsibilities with PaaS

With PaaS, a cloud provider delivers hardware and software tools to clients, typically for an application development environment, via the internet. The service provider hosts hardware and software on its own IT infrastructure, so companies using these services don't need to install their own in-house hardware and software in order to develop or run new applications.

When PaaS is used strictly for development environments, companies still need to have an IT infrastructure, but they rely on cloud providers for key services such as application hosting or development. Clients can install applications and data sets within the PaaS provider's environment, which is optimized for development and testing tasks.

A growing number of organizations, particularly those with limited internal development resources, are leveraging PaaS offerings via the public cloud to gain a reliable and secure application development environment. Among the potential benefits are faster time to market for applications and cost savings from not having to build their own development infrastructure. Also driving growth in the market is the desire among companies to develop new applications in the cloud.

As with IaaS, the service provider handles the management of networks, servers, virtualization, and storage systems, but also oversees management of operating systems. Customers are responsible for data and applications.

The client is also responsible for the security of the environment. That includes data protection, disaster recovery, and data governance at all layers. Although the cloud provider does vulnerability and penetration testing on its cloud network, the client is still responsible for protecting its data and code. Penetration and vulnerability testing, scanning, monitoring, reporting, and remediation still resides with the client.

As with IaaS, it's vital to work with PaaS providers to avoid miscommunications related to management issues.

Client responsibilities with SaaS

SaaS is a software distribution model in which a service provider hosts applications on its own servers and makes them available to clients as needed via the internet.

The model eliminates the need for organizations to purchase, install, and run applications on their own data center systems, and that in turn eliminates the expense of buying and maintaining hardware to support the applications. It also takes away the costs of software licensing, installation, and support.

Among the key benefits of SaaS is the flexibility and cost savings it can provide.

Instead of buying software and additional hardware to support it, organizations subscribe to a SaaS offering whenever they need it, and typically pay for service on a monthly basis based on usage.

SaaS has become an integral part of the IT strategy at a growing number of organizations, as they move applications such as customer relationship management (CRM) and enterprise resources planning (ERP) to the cloud.

With this SaaS model, organizations are still responsible for quite a few management functions. For example, they continue to handle things such as application administration and configuration. They also need to map business workflows to leverage the service, take care of reporting, and manage application data.

Client organizations are also responsible for data governance and cyber security functions such as identity management, controlling which users have access to the application data and how changes in data access are audited.

The integration of the SaaS offering into other systems in use at the organization is also the client responsibility. This can lead to other IaaS, PaaS, hybrid or private cloud infrastructure connections. The data governance, protection, and security of that information would fall on the client once that data is removed from the SaaS solution.

Companies should look to forge a partnership with SaaS providers in which all parties understand their responsibilities.

Summary and conclusion

The key lesson of all this is that management responsibilities by no means disappear when a company moves workloads from on-premises systems to the public cloud, or decides to shift IT infrastructure or development environments to the cloud.

> Some responsibilities will surely go away, otherwise there would be less incentive for moving to the cloud in the first place. Others will be handled in new and different ways.

The public cloud is designed to make things easier from an IT delivery and management standpoint, but it does not free up the IT department from the day-to-day responsibilities of ensuring that reliable technology services and tools are being delivered to users.

Although the public cloud removes some responsibilities, the workloads still need to be monitored and managed. New cloud operational disciplines around cost management, cost optimization, and security change operational requirements of the past. In order to get the most value out of a cloud migration, organizations need to understand and take ownership of their respective responsibilities.

The best way to avoid potential disputes with public cloud providers over management responsibilities is to have a clear understanding of roles well before engaging in IaaS, PaaS, or SaaS. That means thoroughly researching the services that providers are offering, and in many cases enlisting the help of a third-party partner that understands the cloud market.

The cloud in all its forms can be a source of significant benefits for organizations:

+ Increased flexibility
+ Easier scalability, etc.

The cloud model can completely transform the way organizations deliver IT services to end users, helping the business to be more innovative and better serve its customers.

In order to reap the maximum value from these services, however, companies must learn which responsibilities they will hold onto, even as the cloud changes so much about IT.

Getting help and more information

We have helped mid- and large-size organizations navigate to public and hybrid clouds and optimize resulting business value. From developing cloud strategies, assessing workloads, and choosing best-fit cloud platforms, to creating cloud-ready IT governance models, security practices, and service catalogs, we help organizations accelerate smart IT transformations.

Leverage our additional cloud resources for further details:

- Solution brief: Managed Cloud Services
- Whitepaper: "Public Cloud Workload Migration: 9 Common Mistakes to Avoid"
- Whitepaper: "Moving Workloads to the Public Cloud? Don't Forget About Security."
- On-demand livestream event: *Intelligent Technology Forum: Cloud Platform Workload Alignment*
- eBook: "Key Considerations When Migrating Workloads to Public Cloud"
- Video: *Platform and Workload Assessment*

To learn more about us and any specific services available, see the appropriate services web page. Or contact us directly at 800.448.6314.

Meaningful solutions driving business outcomes

We provide expert guidance on cloud integration and data center transformation to organizations of any stage or maturity. By holistically supporting the adoption of new technologies, we enable companies to meet business challenges, improve service levels and efficiency, support growth, and reduce risk.

Learn more at:
datalink.com | insight.com

MTPC-WP-1.0.06.18