WHITE PAPER:

Managing Risk vs. Reward in a Multi-Cloud World

The 18 key factors you need to consider to ensure your long-term hybrid cloud success.

Sponsored by: DELL EMC

OneNeck® IT SOLUTIONS
a TDS® Company

When cloud computing first emerged, people talked about "the cloud" as if it were one big virtual data center in the sky. But as the industry has matured, this revolutionary paradigm has splintered into many varieties — all with unique benefits to today's enterprises. It's no longer one monolithic cloud, but many flavors of service such as infrastructure, platform and software.

These cloud services now reside in many different places, including private and public clouds, on-premises systems and colocation solutions. In short, IT departments now mix and match a variety of different clouds and data center environments, linking them together in hybrid configurations called multi-cloud environments.

In fact, companies today use an average of eight different cloud providers for various applications and services, according to a recent survey conducted by IHS Markit. And by 2019, that number is expected to expand to 11.[1] Similarly, a recent survey by 451 Research found that 69 percent of enterprises will have multi-cloud environments by 2019.[2]

The benefit of having a variety of cloud providers is that you gain a wealth of resources and can run each specific workload on the type of cloud best suited for the applications' needs. This heightens your ability to increase efficiency and lower costs. These various cloud providers open up the possibility of cloud arbitrage, where workloads can be housed in low-cost platforms when needed, then moved to a higher-cost cloud when high-end features are needed. This ability to orchestrate on the fly can be critical to a successful digital transformation strategy.

In addition to offering a broad range of options, a multi-cloud strategy delivers many benefits that make it highly attractive to enterprises today, such as unprecedented cost savings, resource scalability, agility, quicker time to market and improved availability, to name a few.

However, implementing and managing a multi-cloud environment can get complicated fast. Deciding which workloads go where, knowing when and how to move them, balancing costs and capabilities among the various cloud options, and managing resources holistically across the entire ecosystem can be a challenge even for the most sophisticated IT leaders. It can pay big benefits in both the short term and the long term to have a strategic partner support you in the process.

Balancing Business and IT in Multi-Cloud Environments

In preparing and planning for your move to the multi-cloud world, it's important to realize that this shift involves more than just rethinking your IT. A move to a multi-cloud environment can be a massive cultural shift as well. Moving to the cloud continues and extends the trend of moving IT away from a command-and-control structure and toward an on-demand environment where the business can access IT services 24/7 without the need for IT. A multi-cloud environment allows your business decision-makers to move more quickly on opportunities as they arise, to remain competitive in the marketplace.

Yet in spite of this cultural shift to real-time access, IT still needs to control, secure and manage the complexity of a multi-cloud environment. Without it, chaos may cancel out its cost and efficiency benefits. Who has the authority to move workloads, and under what circumstances? Who is responsible for tracking moves and other data to provide an accurate view of the entire system? There are so many different moving parts that data and resources can become fragmented and easily lost in the shuffle.

Indeed, a survey of IT leaders by Forrester Research found that the biggest challenges with multi-cloud strategies are securing data as it moves among different cloud services, tracking costs and usage across multiple clouds, and maintaining integration.[3] This is still the domain of IT.

Dr. Owen Rogers, research director at 451 Research, highlighted the difficulties of multi-cloud. "Cloud buyers have access to more capabilities than ever before, but the result is greater complexity…. The cloud was supposed to be a simple utility like electricity, but new innovations and new pricing models mean the IT landscape is more complex than ever."[4]

The complexity of orchestrating multi-cloud environments can seem overwhelming for any enterprise. However, with careful and thorough planning, followed by astute attention to adjustments to optimize operations, you can gain enormous benefits.

18 Considerations For Successfully Moving to a Multi-Cloud Environment

This paper describes 18 key factors that influence a company's ability to succeed in a multi-cloud environment. These factors are divided into two phases: Architect and Plan, and Operate and Optimize.

The first phase includes the considerations you want to pay attention to up front, to help you plan and structure your architecture into a strategy. The second phase includes factors to consider as you implement that strategy, to help ensure that you derive the greatest benefits—both in the short term and to future-proof your investments.

These factors are not intended to be an exhaustive list. The pace of technology is so rapid that new issues will continue to arise. However, the factors described here can form a solid foundation for a specific strategy that allows you to build as you move forward.

Phase One: Architect and Plan

Before undertaking any transition to the cloud, it's essential to understand its basic fundamentals and what you need to pay attention to. As you plan your multi-cloud strategy and design your architecture, consider the nine Architect and Plan aspects.

1. Security

   Although security should be a priority throughout your transition, you should make an evaluation of your security needs and how various platforms will meet those requirements at the earliest stages of planning. There are both universal and individual security considerations to be aware of. Universally, consider the overarching security you need across your multi-cloud configuration, which may include hyperscale public clouds, hosted private clouds, colocation and on-premises operations. Each of these may provide different levels of security and may even use different types of security tools. Ideally, you want to manage security across all clouds from a single pane of glass.

   Start by finding out what security frameworks various cloud providers use. One of the most common is the Cybersecurity Framework from the National Institute of Standards and Technology (NIST). Will the NIST framework meet your needs? Do certain workloads need to comply with additional, specific security standards? If a workload handles medical data, for example, it needs to be housed in a platform that is compliant with the Health Information Portability and Accountability Act (HIPAA). If you deal with the federal government, you may need to meet the requirements of the Federal Risk and Authorization Management Program (FedRAMP).

   One of the biggest security challenges in multi-cloud is understanding the dependencies among different workloads and data in various platforms. A public-facing webpage that serves up non-sensitive information from a database may be fine in a hyperscale public cloud because it doesn't connect to other databases or other parts of your infrastructure. But if it grabs data from another application that also includes sensitive data such as healthcare records or other personally identifiable information (PII), consider how you can keep that data safe and compliant.

2. Data Moves and SLAs

   Ironically, one of your priorities in the planning process should be to consider your exit from a cloud vendor before you engage with it. If not, you may find that any cost savings from the cloud are lost when you move data. Be sure you understand who owns the data and what fees apply to moving data.

   You also need to understand what would happen if you want to switch to another cloud provider or bring workloads out of a cloud and back into your on-premises data center.

   You'll also want a thorough understanding of each provider's service-level agreement (SLA). Your workloads will drive your requirements, so you'll need to be clear within your own organization about what your service level needs are. Will the cloud providers' availability and uptime assurances be sufficient? Are their SLAs backed by financial guarantees? With all of these considerations, the clearer you are up front, the fewer issues you'll have later.

3. Interoperability

   Interoperability is essential in a multi-cloud environment. How interchangeable are the physical resources used on-premises and those in the cloud? Can your managed service provider (MSP) support bare metal requirements? You may have workloads on your own servers, either in your own data center or at a colocation provider, that you want to use until the end of their life cycle before migrating to the cloud. Will the hosted private cloud provider allow you to attach directly to its infrastructure? Not all of them do.

   Not only must you ensure interoperability at the beginning, you must also consider how you are going to maintain interoperability in the future. Gartner estimates that within two years, more than three-quarters of businesses will be running tools with multiple delivery and operating systems. The firm predicts that about half of these business will need a full-time API manager overseeing the integration of this diversity of systems.[5]

   You'll also need to find out what replication technology is used. There are software utilities that will replicate across platforms and vendors, but not all cloud vendors use the same one. If they don't, how will your data and workloads be replicated or moved among different platforms?

4. PaaS vs. IaaS vs. hybrid solutions

   With increased demand for Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and even Software as a Service (SaaS), knowing exactly which is best for your organization will help you make shrewder IT investments. It may sound fundamental, but there can be misunderstandings over a platform's definition and its services. What are IaaS, PaaS and hybrid solutions all about? And how can you cut through the industry jargon?

   In general, PaaS is a cloud-based platform used to build, test and deliver applications. It's a one-stop shop that allows customers to develop, run and manage applications without

the complexity of building and maintaining infrastructure for those applications. IaaS is pay-as-you-go access to storage, networking and computing resources. It delivers infrastructure on an outsourced basis to support enterprise applications. A hybrid solution is a combination of any of the offerings, such as a mixture of on-premises, private and public cloud services, typically with some level of orchestration among the platforms.

5. Business continuity

Business continuity is your ability to overcome serious incidents or disasters and resume normal operations within a reasonably short period. This is of paramount importance as you move applications and data to the cloud. As with any business, some of your applications have a higher importance than others. Typically, only 20 to 30 percent of an organization's applications are what are deemed mission-critical.

However, to ensure your company's survival, you'll need to make sure your mission-critical workloads are protected for optimal business continuity and disaster recovery. Are they in places that meet your parameters in terms of recovery time objective (RTO) and recovery point objective (RPO)?

Make sure these workloads are segmented and compartmentalized at the application layer, with RTO and RPO specified. For applications that are not as critical, think in terms of what downtime would cost your business and determine an acceptable level of risk for those applications.

6. Controlling cloud risks

The more thought you put into governance up front, the better you will be able to control the risks. One of the biggest risks in cloud environments, especially in the multi-cloud environment, is virtual machine (VM) sprawl. When all it takes to spin up a new server is the swipe of a credit card and the click of a button, it's easy to lose control of both the number of VMs and the associated costs. Consider how you'll govern the process, providing the right access to the right people, thereby reducing the potential for that sprawl.

A second risk is latency. When accessing servers on-premises, users are connected via Ethernet to a data center at the same site in most cases. In the cloud, users are often far away from workloads, and what's connecting them—the internet—can be slow. This can impact user experience for both employees and customers. As you plan your cloud strategy, think about where you need top speeds and where you might trade some degree of latency for lower connectivity costs.

A third risk is loss of hypervisor control. With on-premises virtualization, you have control of the entire infrastructure stack, all the way to the bottom layers of the infrastructure. With hyperscale public cloud, you may only control the operating system level and higher. To mitigate your risks, make sure to understand what level of hypervisor control each cloud offers and if you require that level of access.

7. Access

As previously noted, connections to the cloud over the internet can experience latency. If speed is critical to the user experience and you are willing to pay more, consider a direct, private connection. In weighing access options, factor in the size of workloads, the amount of data to be transmitted, and how often and how quickly you need to refresh or replicate data. It's a good idea to run some tests before deciding. Spin up a few servers in the public cloud, for example, and see how applications perform.

Another aspect of access is the fee that cloud vendors can charge to move data. Many cloud migrations have blown through their budget because of unexpected ingress and egress charges. And don't assume that you won't ever move the workloads. Events such as a new office opening in Germany or a new data sovereignty law in Singapore can change where your data may need to be.

With the possibility that some of your data could be anywhere on the planet, an important security consideration regarding access should be encryption. Do the cloud providers you're considering encrypt some or all of your data? Is the data encrypted during transmission over the internet and at rest? How stringent is access and how is it controlled?

8. Total cost of ownership

Calculating potential total cost of ownership (TCO) before making a move to the cloud or making changes in your current environment is essential. But such calculations may not be very accurate unless they consider all pieces of what can be a complex puzzle. Calculating cloud expenditures can be much more challenging than simply comparing capital expenditures against operating costs.

Make sure to include licensing costs as well as the cost of employees to manage the environment. For example, will the cloud vendor supply its own staff to manage your workloads? If so, you may be able to redeploy your staff to critical internal needs.

Another way to calculate TCO is to adjust for scalability—sometimes you'll be using more cloud capacity, and

sometimes you'll scale it back. Quantifying all of this is, admittedly, often simply guesstimates. Cloud providers can help by supplying their prices, and third-party integrators can provide industry standard costs for some things, such as staff resources. It's also useful to evaluate what costs you will be able to avoid, such as transferring certain tasks and their associated risks to the provider.

9. Migration

Understanding the dependencies among different workloads on different clouds becomes particularly challenging when you start moving applications and data around. Although you can't anticipate all your migrations—after all, the big appeal of the cloud is its agility and flexibility—you should understand the dependencies among resources, workloads, applications and data.

If you move a workload from on-premises to a hyperscale public cloud, will it still perform the same? Will it have the data it needs, or will latency be introduced because it now needs to fetch data from somewhere far away?

In addition, what are your migration options? Will you use software replication, or will you physically transport a server to a new location? Often, MSPs provide migration services, which can unburden your internal IT staff so that they can focus on other essential tasks.

Phase Two: Operate and Optimize

Although the benefits of a multi-cloud environment are clear, the on-demand nature of cloud use can result in uncontrolled costs. This means that it will be important for you to develop a completely new approach to managing and optimizing spend. Here are the nine key aspects to consider as you operate and optimize your multi-cloud strategy for ongoing operation.

10. Security

In the cloud, you don't have to manage physical servers or storage devices. But you will have to manage software-based security tools to monitor and protect the flow of data into and out of your cloud resources. As a first step, determine the best way to manage day-to-day security operations. Will you have a full-scale security operations center (SOC)? If so, how will alerts be handled, and by whom? If you use the SOC of an MSP, determine which alerts you want reported to your internal security team and which you want the MSP to handle.

Next, consider how authentication and access procedures could change when workloads are moved. Most likely, processes in place for on-premises environments won't directly translate to the cloud. Often, another layer of security is needed because employees are accessing data remotely rather than via an internal company network.

Finally, be sure to re-evaluate encryption. Now that you're up and running, you may need more, less, or different encryption. You may also see that encrypting certain data comes at a higher cost than expected and may lead to potential performance impacts as well.

11. Monitoring and capacity

Different cloud platforms use different tools for monitoring and managing workloads. How will you unify these tools to see across all your environments? For example, a hyperscale public cloud may automatically spin up another server when a disk is 80 percent full. In a hosted private cloud, you might move the workload instead. Will you or the MSP perform preventative maintenance to stay ahead of capacity constraints and troubleshoot these items before minor issues grow into major problems?

Different cloud platforms also bill differently. Normalizing bills across platforms to understand true overall cost can be a gargantuan task. Billing from any one vendor can be hard enough to understand. Some IT leaders have actually hired accountants to work with IT to decipher their multi-cloud bills, catch questionable charges and come up with total costs. "It is a nightmare for enterprises to calculate the cost of computing using a single cloud provider, let alone comparing providers or planning a multi-cloud strategy," said Dr. Owen Rogers of 451 Research.[6]

12. Updates and patches

It's essential to devise a patch management process to ensure that the proper preventive measures are taken against potential threats. What cloud environments will be patched, by whom, and how often? Some companies patch applications or upgrade the operating system as soon as possible. Other companies wait to see how a new release is received.

The number of patches required on a consistent basis can be overwhelming. If you take responsibility to do updates and patches, will your staff be available 24/7, 365 days a year? Or will the MSP be responsible for patching and updates during non-business hours to minimize the risk of any type of outage?

When it comes to updates in the cloud, make sure you have a plan for handling problems. If an update corrupts a drive, your ability to restore the data on that drive could depend on your, or your vendor's, ability to find out what was on that drive, how recently it was backed up and where the backup is stored.

13. Multi-Cloud management

Without comprehensive visibility into your multi-cloud environment, you can't consolidate and prioritize fixes, perform audits or know what assets support which part of the business. Applying the same governance and management across multiple clouds obviously helps optimize operational efficiency.

Ideally, you will be able to view all your systems through a single pane of glass. But even if you can't, you can still understand the controls that are in place in each platform and try to make them as consistent as possible. For example, the same person who is authorized to access data on one cloud should be able to access similar or corresponding data on another platform, and certain IT staff could be authorized to spin up new servers on platforms.

14. Governance

When it comes to the cloud, governance plays a vital role in compliance, security, cost control and performance. It can also help you rein in shadow IT, keep an eye on internal and provider SLAs and add accountability. However, governance in the cloud can be different than general IT governance because of the cloud's distributed nature. It is not always clear who is accountable for the cloud service.

There may be governance standards that are particularly suitable for your business, but a common technique is the RACI (responsible, accountable, consulted, informed) matrix, which defines and documents project roles and responsibilities. A tool like this makes crystal clear what the MSP does and what the customer does. In some cases, respective roles and responsibilities are defined by service catalog definitions in the contract. Other standards such as ITIL, ISO or CoBIT can also be useful to align expectations as well.

15. Orchestration and automation

Orchestration coordinates processes across domains, systems and teams, allowing you to accelerate delivery for new innovations, applications and hybrid infrastructure. In your multi-cloud environment, you'll need to figure out how best to manage the different providers to give you the most time-saving and cost-effective solution to keep data management under control.

How will your various cloud platforms work together? They may use standard APIs, but there can still be issues with synchronization. Start by selecting a platform to be the keeper of the truth, the master of record. Information can then propagate from that source to other platforms.

Next, who will run each platform? Because each platform is different, responsibilities may be different. Hyperscale public clouds, for example, run their own automation on their own platforms. In hosted private clouds, it may be shared between the customer and the provider.

16. Workload mobility

An important factor for mobility in the operation phase is the interoperability of hypervisors. If you're running VMware on a hosted private cloud, you may not be able to move it to a public cloud because that platform uses a different hypervisor.

The compatibility of network configurations and connectivity can also be an issue. Will an application that previously ran on the internet run the same way on a private circuit? Figuring out how to manage these and other factors can lead to downtime when you try to migrate workloads between disparate platforms.

You can avoid some of these problems through careful and preemptive planning. If you're spinning up a new device, for example, configure it to run on all the platforms. Even with planning, however, surprises are inevitable. With experience, you'll become better at judging whether moving a particular workload is worth the cost of a possible outage or downtime to execute the move.

17. Managed vs. unmanaged

Businesses today have an expanded set of options for operating in the cloud. For example, you can choose to manage cloud infrastructure yourself or opt for a managed cloud and have an MSP shoulder the burden of day-to-day management. Both managed and unmanaged solutions certainly have their advantages, and which is the best fit for you truly depends on your business.

You'll need to determine how much your company will depend on the services and how much flexibility versus support you will ultimately want from the provider. This requires a familiarity with your company's needs and goals.

The intricacies of moving workloads may also factor into whether you want your MSP to manage those moves, at least at the hypervisor and operating system levels. These providers will offer SLAs for moving workloads, which allows you to transfer a certain amount of risk to a third party and save your internal IT staff for business-critical initiatives.

18. ITIL processes

The ultimate goal of the ITIL standard (ITIL was formerly an acronym for Information Technology Infrastructure Library) is to improve how IT delivers and supports business services. It not only focuses on IT management, but also on improving the capabilities of people, processes and technology. If your service provider is following ITIL best practices, everything will be logged in a change management system. If you also use ITIL, you may be able to "e-bond" your systems. This means that you can integrate the two change management systems, which can provide greater visibility and ease of use.

It's also critical to use operational runbooks, an ITIL best practice that documents systems and practices to be shared with the MSP. When runbooks are well maintained with thorough and up-to-date information, the MSP can quickly address problems that arise at any time, even if your primary engineers are not immediately available.

Succeeding in the Multi-Cloud World

Using multiple clouds from multiple vendors with a mix of public and private clouds is becoming a way of life for many enterprises today. However, as you've seen, operating in a multi-cloud environment is not without its challenges—complexity, resources, expertise, cost and management, to name a few.

When your enterprise is using an amalgam of public clouds and private clouds, managing those cloud implementations is a careful balance and will determine your enterprise's multi-cloud success.

There is no single answer to the question of how to best manage a multi-cloud environment. In general, success with a multi-cloud strategy will require a combination of advanced technology and savvy IT professionals—along with a partnership with a managed cloud services provider.

The 18 key factors described in this paper will help you plan your strategy and put you on a solid foundation in your organization's journey to an efficient, cost-effective and manageable multi-cloud environment. OneNeck IT Solutions offers consultative assessments and advice based on our experience with hundreds of IT projects, including migration to multi-cloud environments, in almost every industry. Our experts provide independent, unbiased recommendations to help ensure that your organization thrives in a multi-cloud world.

References

1. Angus Loten, "CIOs Contend With Ever-Expanding Range of Cloud Services," Wall Street Journal, December 1, 2017 (https://blogs.wsj.com/cio/2017/12/01/cios-must-manage-ever-expanding-range-of-cloud-services/).
2. Nick Ismail, "The multi-cloud/hybrid IT environment will come to dominate the enterprise," Information Age, November 27, 2017 (https://www.information-age.com/multi-cloudhybrid-environment-dominate-enterprise-123469737/).
3. Angus Loten, "Multi-Cloud Strategies Grow, Bring New IT Headaches: Survey," Wall Street Journal, July 12, 2018 (https://blogs.wsj.com/cio/2018/07/12/multi-cloud-strategies-grow-bring-new-it-headaches-survey/?mod=djemCIO_h).
4. Ismail, "The multi-cloud/hybrid IT environment."
5. Loten, "Multi-Cloud Strategies Grow."
6. Ismail, "The multi-cloud/hybrid IT environment."

About OneNeck IT Solutions

OneNeck IT Solutions LLC offers hybrid IT solutions including cloud and hosting solutions, managed services, enterprise application management, advanced IT services, IT hardware and top-tier data centers in Arizona, Colorado, Iowa, Minnesota, New Jersey, Oregon and Wisconsin. OneNeck's team of technology professionals manage secure, world-class, hybrid IT infrastructures and applications for businesses around the country.

OneNeck is a wholly owned subsidiary of Telephone and Data Systems, Inc. [NYSE: TDS]. TDS provides wireless; cable and wireline broadband, TV and voice; and hosted and managed services to approximately six million customers nationwide through its businesses U.S. Cellular, TDS Telecom, OneNeck IT Solutions LLC, and TDS Broadband Service LLC.

For more information call 855-ONE-NECK or visit www.oneneck.com

DELL EMC PARTNER GOLD

Part #WPMCE_0519_V2