



# OneNeck White Paper Transitioning to a Cloud Environment

Analyzing options and leveraging benefits for business-enhancing results

“Cloud computing” is one concept that has moved to the forefront of the market in recent years. As companies deal with increasing demands for IT services and decreasing budgets, cloud computing solutions have gained traction.

But, cloud computing comes in many shapes and sizes. Trying to grasp just what the cloud represents can be mind-boggling. How it’s defined depends on how wide or narrow people see it. In the broadest sense, cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to end user computers and other devices on-demand.

Cloud computing enables businesses to move from working within their own IT bubble and use the cloud to access technologies they need, when they need them, at the scale they need them. Cloud computing offers companies of all sizes creative ways to address how they utilize IT, which in turn frees them to focus on what matters most – their core business.

The key is to bring clarity to the complexity created by this new opportunity and understand how cloud computer fits into your overall IT strategy. You must be able to identify areas for IT efficiency and tie investments directly to a business case with a return on investment proposition. So, before you get too caught up in the cloud frenzy and leap right in, you need to consider some things before transitioning your infrastructure to the cloud.

## ELIMINATING TRANSITION PAIN WITH A LITTLE PLANNING

Every company must weigh the benefits and costs involved in cloud computing. Although the technology is new and the options are somewhat overwhelming, companies basically are deciding whether to “build or buy.” The same assessment an IT manager would make when deciding to build or buy applications applies to the cloud or on-premise decision.

### STEP 1: CLOUD SELECTION

To begin the transition, companies need to identify which of their technologies should be:

- Owned and managed internally,
- Owned internally but managed by a third party,
- Purchased, managed, and accessed through the cloud.

Most organizations will find that picking one type of cloud over another simply may not meet their needs. Often, organizations will pick different clouds for different IT needs. The different types of cloud environments include Public, Private, Dedicated and Hybrid offerings:

**Public Cloud Environments** – Public clouds are built by providers that want to leverage the scale of large server farms and the Internet to bring “on-demand” computing to the masses. User organizations relocate resources such as data, applications and services to computing facilities outside their corporate firewall to these providers. End users then access these services via the Internet, which is shared with other companies; hence the name “public cloud.” Google and Amazon are familiar examples of public cloud providers.

**Private Cloud Environments** – Like a public cloud, a private cloud is built by providers who want to use the scale of server farms to bring “on-demand” computing to their customers. However, private clouds are different than public clouds in that, there is a formal agreement (contract) established between the parties which formally defines the services and commitments between them. The customer is often required to define the length of the agreement, along with a minimum quantity of assets required. Private cloud environments often provide better security options and generally can meet common regulatory compliances.

Not all clouds are created equal. Therefore, you should match a cloud solution to your business objectives. In most environments, cloud computing works best when it virtualizes the entire IT infrastructure. Organizations can manage resources as a shared utility and quickly reconfigure the environment on-demand.

**Dedicated Cloud Environments** – A new style of cloud is now emerging in the market. A dedicated cloud belongs to a single customer, but is being hosted and managed by a provider. This provider has created a private virtual server farm using servers dedicated to only that one customer; no other customers run virtual servers within that farm. While the server farm is not shared with other customers, the service provider may provide storage and backups utilizing storage area networks and backup devices shared by many customers. Dedicated clouds are the most customizable for organizations since the physical assets that make up the cloud environment are literally dedicated to one organization.

**Hybrid Cloud Environments** – These types of clouds combine the features of public, private and dedicated clouds to deliver a single hybrid cloud solution. Using a hybrid cloud platform enables organizations to delegate tasks with specific security or other concerns to a private or dedicated cloud while letting all public operations go to the public cloud segment.

### STEP 2: CLOUD ARCHITECTURE CONSIDERATIONS

The next step is to consider cloud architectural components and compare them to your organization’s needs. It might also be time to correct some IT operational oversights or mature certain processes as part of the transition. It is important to always remember that cloud offerings are not created equal and research on the following topics will save a lot of time, strain and money.

**SLA Management** – Service Level Agreements provide a promise of reliability. To minimize risk, companies need to have SLAs even in places they wouldn’t think they needed them, and they must define what happens in outage scenarios. SLA management applies to all types of clouds whether provided by a third party or owned and managed internally.

**Security Concerns** – Security issues must be weighed as well. How will a company make sure that confidential information remains protected? Could a company's proprietary data be accessed by a cloud provider, or another cloud user, or even worse, a competitor? How comfortable companies feel in the cloud will determine their degree of engagement, and what kind of information they will share and what services they will contract. Trust, in fact, has always been a factor between organizations. When choosing a cloud provider, explore their security processes and procedures thoroughly. Perhaps you want a sense of how they handle security management for their customers. Every cloud provider should be able to articulate security policies and procedures in a formal Security Policy document that can be provided to prospects and customers.

**Change Management and Control of IT** – Change management and the control of IT can present another potential issue. You need to have a clear definition of roles and responsibilities and who is the owner presiding over which systems, management responsibilities and technical processes. Also, ensure your cloud provider aligns with your expectations on a change management process and make sure the collaboration objectives in it are realistic. It is not only acceptable, but often an excellent idea to leverage your cloud provider for managed services should they provide those services. Operating system and application management is often offered by cloud hosting providers.

Migrating to a cloud computing environment can provide organizations access to new services and applications, increased processing capacity, collaborative capabilities and managed services such as data backup and restoration and security. The services are all on demand and at costs often below what individual organizations can achieve.

**Portability** – What if you want to bring an application back in-house? Is there an efficient way to get it back? Companies need an exit strategy and “roll-back” plan. What is the impact to the business when transitioning back in-house? Knowing the options is critical to determining when and how to use the cloud. Migrating applications from physical servers to a cloud infrastructure can involve changes to the operating environment and the application itself that can make it difficult to ‘roll-back’ if not discussed ahead of time. If working with your cloud provider, make sure they have the tools in place necessary to allow you to return an application to its original state. Should you want to migrate from one cloud provider to another, ensure your servers are not in a proprietary operational format that would limit your options for future transitions.

**Compliance** – Compliance raises other questions. Who owns the data? How is the data affected by being hosted in regional locations? What about government efforts to claim ownership or access to data stored on a cloud provider? And there's the issue of how all this may be affected by government regulation, such as the Sarbanes-Oxley Act. What about other compliance requirements and tracking process

for regulatory reporting? How will the experience in the cloud allow for fast audits and the ability to respond to government inquiries within mandated timeframes? Do they have a SAS 70 Type II or equivalent? Do the controls apply to the cloud architecture? Does your organization require PCI compliance and does their offering in the cloud provide the necessary regulatory compliance. Your cloud provider must be able to meet your compliance needs. Data ownership isn't usually a concern unless you are working within the confines of a public cloud. Make sure you have compliance issues worked out prior to any transition.

**Integration** – One factor not often considered when evaluating cloud computing is ensuring application integration across data centers. It's one thing for an individual or department to subscribe to a cloud service. But that poses significant risk of creating technology and business process silos. Some cloud vendors provide for application integration in their offerings, others do not. The key point companies must remember is to assess their ability to integrate both their applications and business processes around the cloud solutions that they adopt on and off premise.

**Transparency** – How do you know you have met your service level agreements? How do you measure your uptime? What metrics are available to help you plan and budget for growth in the future? These are all questions that deal with transparency in the cloud. Most cloud providers offer some level of real-time monitoring and reporting of the cloud infrastructure that you can access via a portal. A mature cloud offering will include dynamic and historical reporting, alerts and trending analysis for your IT organization's consumption. The information should be clear and easy to read.

**Business Continuity/Disaster Recovery** – Transitioning to the cloud can be an excellent opportunity to finally get a true disaster recovery solution in place for your organization. By design, the cloud inherently offers advantages to ease organizations into disaster recovery option, often with low RTO and RPO obtainment for relatively modest costs. If transitioning to the cloud, now is the time to identify your mission critical applications and services for your business and ranking them for disaster preparedness. Several cloud providers spread their cloud infrastructure across multiple data centers and often have wide area networks capable of connecting your users to the environment at multiple points to ensure uptime in the event of a disaster. Even if you are not ready to complete your disaster recovery planning now, you should consider cloud providers that have options to make it easy to meet your disaster recovery objectives in your organization's future.

**Skills** – Companies need to be aware of the skills required to build applications that run in the cloud. In many cases, developing cloud applications require different technology skills than what companies may have in their IT staff today. When planning for the cloud, companies need to understand and assess the impact that cloud vendor selection may have on their existing IT skills, and how they've traditionally built and managed systems. Understanding how your transition to the cloud could affect your IT operational personnel is important. It is a solid strategy to validate that your cloud provider aligns with your IT operational model (i.e.: ITIL) or, if your IT operations are fairly informal today, perhaps use the transition to the cloud as an opportunity to align around one.

### STEP 3: TRANSITIONING CONSIDERATIONS

**Transition Management** – Often migrating to the cloud means significant effort and organizational planning too great for existing personnel to absorb. Communications with end users and executive management, maintenance window planning, application vendor coordination, WAN performance validation, pilot/proof of concept testing, roll-back planning and quality assurance testing are all examples of items that will potentially need to be handled during your transition to the cloud. Should you have several systems and applications to transition, a phased approach may be necessary. Planning and coordinating all of these activities will take project management resources. Selecting a cloud hosting partner that provides project management and oversight and expertise can be truly indispensable. Unencumbered by internal politics and existing operational artifacts, a project manager will work to hold resources accountable to deliverables and provide a conduit for consistent communications and planning.

**Migration Methods** – There are numerous methodologies to consider when migrating applications and systems into the cloud. Typically, your initial planning meeting with your project manager and cloud provider will include discussions on migration methodologies. It is important to understand each type and weigh the benefits and concerns of each.

- **Greenfield** – A Greenfield build is one that lacks any constraints imposed by prior work. For a cloud transition, this could mean setting up new servers and networks in the cloud and then installing applications and data fresh. In organizations that are experiencing a large number of IT related issues that have not or cannot be resolved thru normal systems administration a Greenfield deployment may be recommended.
- **Forklift** – This approach is exactly what the title implies and is the fastest migration when it comes to simply relocating the environment into the cloud. A forklift migration is generally used when the existing IT infrastructure was built using industry best practices and is in good working order. Planning and pre-migration testing, especially data backups, is a critical step prior to making the actual migration. Commonly, a process known as a P2V (physical to virtual) migration is used to move applications running on physical server assets into the cloud

**Network Connectivity** – When transitioning to the cloud, you will need to establish connectivity between your users and the cloud provider. Often this can be accomplished thru VPN tunnels over the Internet however larger scale deployments may benefit from direct, high-speed connectivity. This is especially important if you are linking an existing data center with infrastructure to the cloud provider. Application dependencies over the network must be addressed carefully for the cloud to be effective.

**Ensuring Data Integrity** – When data moves to the cloud, it moves beyond the reach of tools and mechanisms you may have put in place over the years to preserve data integrity. Ensuring that your organization's intellectual property is properly backed up as soon as

a transition is completed is paramount. You'll need to make sure that the cloud provider has a robust backup methodology and offers you transparency into the reports showing backup job completions and failure.

The cloud selection process is not to be taken lightly. Companies should consider a variety of implications and tradeoffs carefully before making a move to the cloud. Prospective cloud customers should take into account the criticality of the software, data or services in question and how they will be protected.

**Managing Multiple Environments** – After transitioning your applications to the cloud, you'll find another potential hurdle: how are you going to manage them? The cloud and your existing IT infrastructure are currently two completely separate environments, each with its own set of system management tools, and often no meaningful way to integrate the two. Your IT staff will need to learn and use each cloud provider's management tools and policies, in addition to the ones they already have. One solution is to have the cloud provider manage the cloud infrastructure including the operating systems and applications. Many cloud providers offer robust managed services for your systems with a competitive SLA.

### CONCLUSION

The key to successfully leveraging cloud computing is addressing pressing issues and keeping expectations in check. Companies must sift through the hype and be realistic about what cloud computing can deliver in terms of ROI, cost reductions, revenue increases and other promises.

Before businesses get caught up in a full-blown cloud transition, it's important to understand what issues cloud computing solves and how difficult the transformation can be without a clearly defined objective at the outset. As with all IT initiatives, every organization needs to align technology strategy with business requirements.

As the industry goes through what some analysts believe will be significant consolidation with cloud, it makes sense for companies to partner with firms that have credentials, broad application platforms and a proven track record in navigating new and emerging technology platforms and strategies.

With cloud computing, the burden of creating, developing and sustaining the entire infrastructure unilaterally gets lifted from a company that may be shouldering it unnecessarily. And if serious problems arise, cloud access provides opportunities that could help the business leverage more affordable and robust disaster recovery options.