The Risk of Lock-in with Cloud Computing

Cloud computing offers the next level of IT capabilities to agencies. When you implement cloud computing, you can adapt to changes in demand and requirements much more quickly than with traditional computing technologies. However, for all of the advantages that cloud promises, there's a downside. There are significant risks associated with cloud computing; the obvious risks of security, data sovereignty, fault tolerance, disaster recovery, etc. – and some not-so-obvious risks.

There is a significant risk of getting trapped in a particular cloud implementation. This is true whether your cloud is providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), but the risk increases as you progress from delivering IaaS to PaaS and SaaS. With IaaS, the largest risk comes from being tied to a particular hypervisor. While today there is one predominant hypervisor in the marketplace, there are many alternatives available – and they're rapidly gaining market share. In fact, one of the largest, most well-known cloud providers does not use the market-leading hypervisor to enable their infrastructure. There are currently two virtual disk formats that are in widespread use: .vmdk and .vhd. Other formats exist, but these are the predominant formats, and it is highly unlikely that there will be a convergence any time soon. To prevent hypervisor lock-in, there needs to be wide-spread adoption of standardized disk formats. The Open Virtualization Format (OVF) is a step in the right direction, but OVF merely provides metadata that describes how to construct a virtual machine (networks, CPUs, RAM, etc.) and provides a record that describes the capacity and format of the virtual disks. The standard does not require a specific disk format – or even that the format specified be able to be converted to a standardized format. All in all, IaaS provides the least opportunity for lock-in, mainly because there are fewer areas where standards are important.

Moving a step up the cloud hierarchy brings us to PaaS. With Platform as a Service, the cloud service provider incorporates additional capabilities into their offering to enable customers to make more efficient use of the cloud resources. These capabilities often include things such as database, security, scalability and messaging services. The inclusion of these services can greatly simplify the development of applications, but they can also serve to keep you tied to the provider's underlying platform. Imagine you have developed your mission-critical line of business application to make full utilization of the cloud provider's extensions. Now, imagine that the provider goes out of business or otherwise becomes unable to meet your demands – or, perhaps, you become dissatisfied with the

level of service or the price ou're required to pay in a few years. How do you move to an alternative PaaS provider?

Without standards for these critical middleware services, you may soon find yourself at the mercy of your cloud service provider, with no real way to escape without devoting a lot of additional, unbudgeted time, resources, and funding in the effort.

This is true even if your cloud is purely private, with all functionality contained inside your organization. In that case, you may be your own provider, and your users could very well be the ones displeased with the quality or inflexibility of your private cloud. How will you ensure that you have an exit strategy for your own implementation?

Finally, let's take a look at SaaS. This is the "holy grail" of cloud computing. With SaaS, you turn over complete control of the infrastructure, all the way up through the application, to your cloud hosting provider (or you assume complete control if you offer your own private cloud). SaaS becomes a "black box" for your users. With SaaS, the days of implementing customized business processes via extensive customization are gone. That's both good and bad: it's good because it enables much more rapid implementation of automation systems; it's bad because your organization loses much of the ability to fine-tune services beyond what's already been decided as part of the SaaS implementation.

With the current lack of standards at each of the cloud tiers, maintaining a high degree of flexibility is a challenge. The chances of becoming "cloud locked" are extremely high. Once you commit to a particular cloud vendor, it can be extremely costly and difficult to pull your systems and data to move to another provider to take advantage of unique capabilities or more favorable pricing models. The implementation and wide-spread adoption of standards at each of the tiers in the cloud hierarchy is essential to ensure the portability of workloads and data among a variety of cloud providers.

Until standards for IaaS, PaaS, and Saas become pervasive among a majority of cloud providers, you may want to consider implementing a private cloud so as to reduce the risk of lock-in. You won't eliminate the risk that your own decisions might not work out, but you won't be at the mercy of anyone but yourself if you need to re-think your design or move in a different direction.

Source : http://kensvirtualreality.wordpress.com/2012/10/13/the-risk-of-lock-in-with-cloud-computing/