Bringing the Cloud Down to Earth

8 Common Misconceptions Life Science Companies have when Considering the Cloud

Presented by MethodSense, Inc.
in collaboration with
HolyCow Branding

Advantages of the Cloud for Life Science Companies
Cloud computing and virtualization is an evolving paradigm that is transforming the way we do business. The economy of scale the cloud provides reduces costs and increases operational efficiencies that reap major benefits. This operational shift can be intimidating for Life Science companies; however, there are significant advantages for moving to the cloud:

- Maintains compliance across multiple applications more efficiently
- Scales up and down with ease
- Provides a platform for collaboration and resource pooling
- Unifies your infrastructure for end users
- Increases the control, availability and flexibility of your data center
- Reduces computing maintenance costs and, depending on the model, can reduce hardware costs

While these advantages are enticing, it's critical that Life Science companies understand some common misconceptions of the cloud before adopting it as a new technology strategy. This article addresses these myths to protect businesses considering a move to the cloud.

A word of advice: The challenges of implementing cloud computing for life science companies have been highlighted by recent publications from IEEE, CIO Magazine and others by observing the absence of accepted standards for the cloud. Before delving into cloud computing for your Life Science company, be certain you have the proper skills on hand to help you. Missteps and short cuts in the path to regulatory compliance typically create additional and unnecessary expenses down the road. MethodSense has helped many clients in this regard.

Misconception #1: All Cloud Environments are the Same
According to the National Institute of Standards and Technology (NIST), there are actually four types of clouds, and each is intended for different use.

Private: This infrastructure is for exclusive use by a single organization. It is only used by its owners, making it the most secure environment. It may be owned, managed, and operated by

the hosting organization, a third party, or a combination of them, and it may exist on or off premises.

Community: This system is for exclusive use by a specific community of users from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of them, and it may exist on or off premises.

Public or Vendor: This infrastructure is for open use by the general public. They are shared among multiple subscribers. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Because of the nature of public clouds, this architecture may present security, privacy and auditing issues.

Hybrid: This cloud type is a composition of two or more distinct infrastructures (private, community, or public) that remain unique entities, but are connected by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Hybrids can be used in the Life Sciences when a combination of regulated and non-regulated information is shared.

As a general rule, a *private* cloud can be effectively adapted to satisfy the stringent compliance needs of a Life Science company.

Misconception #2: Private Virtual Cloud Configurations are Proprietary to the Data Center

We frequently hear cloud providers talk about proprietary configurations or operational trade secrets. Without debating the veracity of such claims, it is important to find and work with a vendor who can share, and work with you, when you are evaluating your cloud options. When a provider understands your needs and why your controls are important, we have found most providers are more relaxed about their "trade secrets" in favor of winning your business. Privacy, security and other controls should be collaboratively implemented with your provider so you can remain compliant. Carefully plan the security and privacy aspects of your cloud environment in partnership with your provider before implementing your solution.

Misconception #3: A Data Center's SAS 70 Type II Certification can Replace an Onsite Audit

The proliferation of professional hosting companies, and subsequently the cloud computing services they provide, has created a competitive environment where service quality can be a competitive advantage. Many hosting companies seek a SAS 70 Type II Certification to demonstrate their quality. However, the audits performed in pursuit of SAS 70 Type II Certification are paid for by the vendor, often focus on security issues, constitute a snapshot of the vendor which may not be relevant to the timing of your contract with the vendor, and the audit may not sufficiently cover your Life Science regulatory concerns. For the criticality of your business, you should sponsor the audit, ensuring you've adequately fulfilled your regulatory requirements. Be prepared, however, to massage and coax the understanding of the vendor for cooperation before and during the audit. In our experience,

© MethodSense, Inc. 2012

most cloud providers focus on the acquisition of Life Science clients with little to no understanding of the regulatory environment we operate in.

Misconception#4: A Cloud cannot be Managed as an Autonomous, Independent System
Your cloud environment can be affected by the configuration and set up of other systems. There are other factors within the data center that may influence your operation: a vendor's performance, upgrades to a vendor's system and overall testing of general "cloud" components. In essence, your cloud consists of your vendor's hardware, firewalls, raw data storage, networks and supporting applications. Even though you may use a private cloud, that network is still dependent upon the vendor's underlying systems.

You must understand the total environment of your provider to ensure your cloud is secure and will remain secure if they make changes to it. The best way to proactively implement your cloud solution for long-term success is to perform a thorough risk assessment at the onset of your transition. A proper risk assessment will lead to identifying the controls that will secure your network regardless of your vendor's behind-the-scene activities.

Misconception #5: The Data Center's Procedures are Enough
While many data centers take the initiative to implement quality systems, SOPs and other quality measures, that doesn't guarantee they will meet your quality management system expectations. Your cloud provider may need to make existing processes and procedures more robust and in a way that is more collaborative than they originally intended. This kind of flexibility should be incorporated into your vendor selection criteria.

Misconception #6: Maintaining your Cloud in a Validated State is Impossible
As long as you've understood the impact the provider's systems and infrastructure have on your validation strategy, then you can create controls to ensure your private cloud remains in a validated state. Anticipate the need to collaborate with the cloud provider on change controls with the introduction of hardware or software modifications. Again, you can set these expectations, and probably garner more cooperation, if you incorporate such considerations into your vendor selection criteria.

Misconception #7: A Cloud Environment does not Allow the Segregation of Information
As mentioned in Misconception #1, there are a variety of cloud environments. Private clouds are the best solution to manage data in regulated industries. They give you the most control and security because you can limit who has access to your computing environment.

With a private cloud you're also able to set up different channels for each information group and create boundaries with respect to your regulated information. These channels allow you to "segregate" your data, establish controls and set permissions. Virtual machines can also serve a similar purpose.

Misconception #8: FDA Regulations Related to Validation do not Apply to Clouds
A third party hosted cloud environment does not excuse you from regulatory obligations that would otherwise exist if you were hosting the services inside your company. The same goals and strategies you apply to your local infrastructure should be applied to your cloud environment. FDA

© MethodSense, Inc. 2012

regulations can be met; you just have to be aware of the applicable risks, the controls for mitigating those risks and the right partner to assist you.

Conclusion

Because you are ultimately responsible for your data's authenticity, veracity, and security, establishing compliance boundaries and conducting periodic analysis of the technology environment is imperative. Be sure to define your validation and regulatory requirements so they apply to your cloud solution.

Whether you are an early adopter or are fighting virtualization every step of the way, cloud computing is here to stay. Shifting your technology operation to the cloud includes benefits, such as:

- Improved scalability, both up and down
- Increased access to and utilization of key business assets
- Improved controls on security and data access
- Increased innovation due to collaboration and availability of resources

Although cloud computing isn't without it's difficulties, it's definitely a viable option for Life Science businesses. To ensure a successful implementation:

- Perform a complete vendor audit
- Outline the operational processes and procedures of your cloud environment
- Identify any major security and privacy risks
- Consider business, financial, compliance and intellectual property risks
- Document risk management strategies
- Provide recommendations to improve the security and on-going compliance

About MethodSense, Inc.

MethodSense is a Life Science consulting firm that helps clients deliver medical and technological breakthroughs by effectively meeting the requirements needed to bring their products to market. We guide medical device, biotech and pharmaceutical companies with quality, regulatory and technology solutions. Our guidance enables clients to operate more effectively during the commercialization process and beyond. MethodSense is located in the heart of Research Triangle Park, North Carolina – home to one of the world's largest biotechnology clusters and a hub for technology-based innovation. We invite your communication: Russ King, (919) 313-3962, rking@methodsense.com, www.methodsense.com.

About HolyCow Branding

Holy Cow Branding is a strategic branding agency located in Raleigh, North Carolina. They emphasize the qualities that differentiate their clients from the rest of the herd through a process that involves developing brand strategy, building brand awareness, creating brand assets and analyzing the results. Holy Cow's clients count on them to help launch new products, revitalize established brands, and to create engaging brand experiences. Contact Lorana Price, (919) 342-3349, lorana@holycowbranding.com, www.holycowbranding.com.

© MethodSense, Inc. 2012