White Paper: Vendor Selection for Your Life Science Company Cloud

GlobalSubmit
123 South Broad Street, Suite 1850
Philadelphia, PA 19109
www.globalsubmit.com

Methodsense, Inc.
P.O. Box 110352 Durham, NC 27709
p: 919.607.4776
www.methodsense.com

Vendor Selection for Your Life Science Company Cloud

By: Russ King, President, Methodsense, Inc. and Jason Rock, Chief Technology Officer, GlobalSubmit

Introduction: What are the benefits of a Cloud?

According to the National Institute of Standards and Technology, the cloud is ña model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.ò

Most companiesôIT infrastructure use less than 30% of their capacity. It took years to get the capacity to where it is today, and it takes months to increase capacity. Employing qualified resources to maintain such an infrastructure is difficult and expensive.

Cloud providers utilize about 65% of their capacity and can add capacity quickly. In short, cloud providers benefit from economies of scale, which enables them to lower individual usage costs and centralize infrastructure costs. Companies benefit by only paying for what they consume. Companies can increase or decrease their usage rapidly, and can spend less time managing complex IT resources.

Not only do efficiency improvements reduce costs, the nature of some costs can change from being capital investment in hardware and infrastructure (CapEx) to a pay-as-you go (OpEx) model. Maximizing IT capacity utilization, improving IT flexibility and responsiveness, and minimizing cost are not the only advantages of the cloud.

Collaboration can be one of the most important advantages of cloud computing. Multiple users, from around the world, can collaborate more easily on documents and projects. Because the information is hosted in the cloud, and not on individual computers, business owners can collaborate with external stakeholders in a secure environment with nothing more than an Internet connection and some identity management controls.

The most surprising benefit of the cloud is security. Top cloud providers have the best infrastructure and security technology with the top people maintaining that infrastructure and technology. Speaking before the House of Representatives, Army General Keith Alexander, commander of U.S. Cyber Command and Director of the National Security Agency, said cloud computing provides the best way to secure DOD networks. As Jesse Lipson pointed out in a recent Forbes article: ñMost cloud computing companies are like experienced airline pilots. They are well trained, have backup systems and contingency plans in case they encounter an issue, and

they have a full staff of professionals regularly checking and maintaining their service. Cloud software companies, knowing the implications of a crash on their businessô bottom line, invest significant resources into ensuring that such a disaster never occurs. Cloud computing companies can invest far more resources in data backup and security than your business can.ò Compare this to the levels of protection that your company provides.

Why do I need to choose the right Vendor?

- **The vendor holds your most critical assets.**
- **Your Electronic Assurance obligations do not change just because you migrate to the cloud.**
- **What can occur if you choose the wrong vendor?**

While the cloud can be a compelling option for life science companies, understanding the risks associated with vendor selection is a critical first step. Cloud vendors often view life science companies as attractive clients because of their long term data management needs and the general belief that life science business delivers a premium for services that can quickly boost margins. But, all too frequently, Cloud Vendors are unprepared for the critical data management needs of life science companies within the context of FDA regulations. The gap, framed by the Cloud Vendorôs strong desire for life science business, the vendorôs frequent lack of knowledge about regulatory requirements, and the perennial pressure on life science companies to control expenses, creates a recipe for short cuts and their associated risks.

The risk associated with a Cloud Vendor choice is directly related to the criticality of the data managed. At the end of the day, the value of a pharmaceutical, biotech, or medical device company is instantiated in intellectual property. This includes the information that satisfies the requirements of the FDA, as well as the requirements of potential commercial partners or buyers. If your intent is to place your critical information in the cloud, then any risk created in your relationship with your Cloud Vendor directly reflects your willingness to potentially compromise your intellectual property and its valuation.

The most frequent risk we see is allowing the priority of regulatory requirements to erode under the misconception that sophisticated data centers and technically savvy Cloud Vendor staff can compensate for, or somehow replace, the intent of FDA requirements to maintain data integrity, authenticity, and non-repudiation. Migrating critical data to the cloud does not excuse you from regulatory obligations that would otherwise exist if you were hosting the services inside your company. The same controls you are required to apply to your internally hosted infrastructure must be applied to your external cloud environment, which means partnering with a vendor that is willing and able to support these controls to the degree needed.

Validating computing environments, virtualized services and systems, security controls, and the actual migration to the cloud are required for compliance. Moreover, maintaining a state of compliance must take into consideration the Cloud Vendorôs tools, systems, practices, and procedures, and, most importantly, compensate for gaps between what the Cloud Vendor has in place and your regulatory obligations. The real risk is realized when either regulators or potential partners have problems with the lack of controls to ensure data integrity and other electronic assurance information values. Without such controls, you may not be able to sufficiently demonstrate the veracity of your intellectual property claims, which directly impacts the value of your IP and commercialization strategy.

A Common Scenario:

A Cloud Vendor sells private cloud services to a pharmaceutical company who subsequently performs a vendor audit on the Cloud Vendor. The audit produces a gap analysis with observations and a commitment from the Cloud Vendor to resolve critical observations against an agreed upon time line. The pharmaceutical company begins migration to the new cloud by validating the virtualization of their systems and then validating the migration to the cloud. As the due date for observation remediation approaches, it becomes apparent that the Cloud Vendor cannot, or will not, address the critical observations on time. The pharmaceutical company must then decide whether they will take on the work and cost of correcting the problems, or choose another vendor, whereby both alternatives threaten the anticipated savings the company thought they would enjoy. Choosing the right vendor from the onset helps mitigate this risk.

Four Guiding Considerations for Cloud Vendor Selection:

Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs which are migrating applications to a cloud environment. NIST defines the cloud deployment models as follows:

- **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized

or proprietary technology that enables data and application portability (e g , cloud bursting for load-balancing between clouds).

Choosing the correct deployment can depend on who needs to access the service, budget and security concerns.

Private clouds are the most secure and most expensive. Private clouds allow companies to have isolated sections of a cloud where you can launch resources in a virtual network. You can have complete control over your virtual networking environment and place your backend systems, such as databases or application servers with no Internet access. You can limit access to these servers based on access control, physical hardware, and IP address. A Private Cloud is therefore mostly suited for sensitive data, where the customer is dependent on a certain degree of security. Private Clouds, to an extent, lose the economy of scale compared to a Public Cloud.

Community clouds spread costs over fewer users than a public cloud. This option is more expensive but may offer a higher level of privacy, security and/or policy compliance.

Public clouds are the least expensive deployment. When most people think about cloud computing, they think of a public cloud deployment. All resources are shared but can be secured. If you are comfortable with the level of security of your cloud provider or have budget constraints, public clouds are your best option.

Hybrid clouds are the typical deployment model for most enterprises. In this cloud deployment model, an organization provides and manages some resources in-house and has others provided externally. The main benefit of the hybrid cloud is that it provides the scalability and low costs of a public cloud without exposing mission-critical applications and data to third-parties.

Know what your privacy, security, and disaster recovery control needs are in advance, and choose a Cloud Vendor that can meet and support your needs.

When it comes to comes to privacy, security, and disaster recovery, you need to first determine your requirements and budget. The Cloud provider can provide you tools to help protect your data, but you need to implement those tools. For example, Cloud providers can allow you to limit access to your data based on their physical machine or location; but you need to remove those access rights when machine or location no longer needs access.

Your Cloud provider needs policies, processes, and control activities for the delivery of each of their services. The collective control environment encompasses the people, processes, and technology. Your Cloud provider needs well trained staff that has limited physical access to your data and processes that protect your data and technology by keeping prying eyes away from sensitive areas. Accordingly, you should choose a Cloud vendor that maintain proper certifications like SAS 70 (the Statement on Auditing Standards No. 70), ISO/IEC 27001, and FISMA.

You also need to ensure the Cloud provider stores your data in the proper region. The selection of a region within an acceptable geographic jurisdiction to the customer provides a solid

foundation to meeting location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive.

You need to have proper disaster recovery controls in place. A traditional approach to disaster recovery involves different levels of off-site duplication of data and infrastructure. Critical business services are set up and maintained on this infrastructure and tested at regular intervals. The disaster recovery environmentôs location and the source infrastructure should be a significant physical distance apart to ensure that the disaster recovery environment is isolated from faults that could impact the source site. Accordingly, it is important that your Cloud provider has data centers located in different physical locations and are isolated from faults from the other data centers. When dealing with a disaster, itôs very likely that you will have to modify network settings as you are failing over to another site. For the most critical systems you want to choose a Cloud provider that will allow you to automate the changing of the network settings.

Although the Cloud provider is responsible to maintain the infrastructure, it is still your responsibility to test your disaster recovery plan.

Choose a Cloud Vendor who understands Quality Management Systems and is willing to partner with you to meet your Life Science QMS needs at the time of implementation and maintain your needs going forward.

Cloud vendors commonly implement quality measures ranging from verbally shared processes and practices to SOPs and trouble ticket software to highly structured Quality Systems. However, advertising a level of quality management does not guarantee that the Cloud Vendor will meet your *life science* quality management expectations. To meet your compliance obligations, 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. Be aware that many Cloud Vendors consider their services to be proprietary and comprised of trade secrets, which may make collaborating around quality more difficult.

Select a Cloud Vendor who can support your Vendor Management obligations.

When selecting your Cloud Vendor, be sure they support your vendor management obligations. Cloud vendors who rightly take pride in their SAS 70 Type II certification, for example, often mistakenly insist that the certification should satisfy all quality and auditing needs. These certifications frequently focus on security issues and may not sufficiently cover life science regulatory concerns. Life science companies face validation requirements and regulatory concerns that go above and beyond SAS 70 certification, such as installation qualifications, change control, audit trails, electronic signatures, and permissions configuration. These requirements should be defined for the cloud environment and services and then implemented in your Service Level Agreements.

Be prepared to massage and coax the understanding of the vendor for cooperation before and during this process. By educating the Cloud Vendor about your requirements, youôll be much more likely to complete a successful migration to the cloud.

Conclusion: Your Cloud Vendor needs to be a partner who fits into your regulatory and quality framework.

Shifting your technology operation to the cloud can garner many significant benefits including:

- Improved scalability and cost savings
- 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

However, regulatory burdens are not abated by shifting to the cloud, and Cloud Vendors today are by and large unschooled on FDA regulations, which, if not addressed, can create risk. Life science companies should select a Cloud Vendor with the expectation that many will depend on coaching and assistance in order to meet regulatory requirements. The Cloud Vendorôs ability to accept and then in a timely fashion respond to your regulatory requirements should, therefore, become a highlighted vendor characteristic in your vendor selection criteria.

Want to know more?

Call at 888-840-9580 or contact us at sales@globalsubmit.com or 919-313-3962 or info@methodsense.com.

About GlobalSubmit

GlobalSubmit is a products and services company that provides transparency in regulated healthcare products. The U.S. Food & Drug Administration and leading Life Sciences companies use our flagship applications, REVIEWÊ and VALIDATEÊ, to review and validate electronic submissions. GlobalSubmitôs thought leaders lead international efforts, constantly working with industry and government agencies to standardize product and study information. The company is headquartered in Philadelphia, Pennsylvania.

About MethodSense

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 ï home to one of the worldôs 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.