Reprinted from
PHARMACEUTICAL ENGINEERING
THE OFFICIAL TECHNICAL MAGAZINE OF ISPE
JANUARY/FEBRUARY 2014, VOL 34, NO 1

www.PharmaceuticalEngineering.org

Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity

by the GAMP Cloud Computing Special Interest Group (SIG)

This article presents the current issues facing adoption of cloud computing, paradigm shifted needed and a strategy for establishing guidance within the pharmaceutical industry.

We are in a challenging time for most traditional pharmaceutical companies; the competiveness of the market place, loss of patents, increasing international regulatory requirements, downward pressure on health care costs. These are just a few of the factors that are driving pharmaceutical companies to adopt strategies of previously never seen cutting of resources and costs that have been present in other manufacturing sectors for some time.

At the same time, IT needs to support the challenges the businesses are facing and are consequently being asked to deliver effective solutions, while cutting costs without compromising quality, compliance, agility and flexibility.

More recently there has been a new term introduced into our IT vocabulary that is causing a great deal of discussion and debate throughout much of the business world - cloud computing. The promises of cloud computing are certainly considerable: extremely fast and flexible solution delivery, on-demand scalability, high-demand business continuity services with easy solutions for backup and archiving. All this, and at a cost which is considerably lower than the traditional internal setup. Is the dream becoming reality? Are IT managers able to meet the speed of delivery and cost pressures of their businesses? Will cloud computing provide the capabilities and adoption levels, while simultaneously meeting the regulatory compliance needs that are core to the pharmaceutical sector?

The dream is not attractive to IT departments alone. IT cloud providers are directly accessible to the pharmaceutical end user. Privately we store our lives on the cloud, our music, our pleasure reading, and our family photos. The next step of embracing the technology in our professional lives is a small one conceptually, but massive if compliance, security and integrity are to be maintained. An end user can engage a cloud provider with a credit card and fix a problem that needs resolving with little or no guidance on how the cloud IT world is different from the environment within their corporate network.

The Reality

Despite the promises of efficiencies and flexibility, there is a very slow adoption of cloud solutions at an enterprise level in the regulated environment. On evaluation of this remarkable phenomenon, we believe the reason is simple – the everlasting dilemma of innovation versus compliance. Our understanding of how to operate today has been shaped in the relatively recent past based on regulations, such as FDA Part 11, EU Annex 11, and industry forums like ISPE GAMP®. As an industry we are holding our breath and waiting for specific guidance around a technology which is still evolving. The longer we wait, the further we seem to fall behind. The absence of specific regulatory guidelines for the cloud, in combination with a very conservative mindset and a historically risk-adverse culture is once again slowing down the pharmaceutical

industry in the adoption of new technology.

So, what is stopping us from simply taking the well-established industry guidance – such as GAMP® 5 and shaping it to fit the cloud computing model? After all, as IT delivery departments, we have adapted GAMP® 5 to ensure our own internal infrastructure and applications are compliant. Would it not make sense to simply create parallel processes for an IAAS, PAAS or SAAS provider like we also did for specific areas such as manufacturing execution systems or laboratory equipment? Can regulated companies accept less than traditional execution of IT controls when considering a cloud provider?

The answer to this question has to be sought in the fact that cloud providers have diverse customer bases – ranging from individual users that simply want to save some files on a central internet location to large multinational companies in a wide range of industries. The representation and importance of the pharmaceutical market in a cloud provider's overall customer base is limited. The limited presence results in limited power to dictate how the quality aspects of the cloud businesses are run. One of the best examples of such a limitation is the fact that some of the larger cloud providers (and the more cost effective ones) are unwilling to open up their companies and processes for scrutiny by multiple teams of auditors. Vendors that do open their doors to audits do not always understand the need for individual regulated companies to audit and would prefer that they could provide these regulated companies a "GxP certification." However, such certifications do not exist.

A second reason that holds us back from embracing cloud systems in the same way as any other computer system is the fact that some of the quality related processes used by the cloud service providers are a little "different," in other words, a bit more risk-tolerant than what we are used to in the conservative pharmaceutical world. The differences can be found in all parts of a provider's organization. What does a "proper" Quality Management System (QMS) look like? If the QMS has all the right elements, is it okay that the QMS is posted on a Wiki and not in an electronic document management system? Do we need to see paper to demonstrate hardware and software is qualified? Does the paper make a server more reliable? Is the QMS on a Wiki, although different from what we have traditionally seen, inferior in any way? The answer is neither no nor yes, but rather 'it depends.' It depends on what the corresponding risk is, how the risk is related to the overall process, and how we can manage and even mitigate the risk on the side of the pharmaceutical company if warranted.

If processes are different at a cloud provider, those responsible for the assuring processes are sufficient (for example Internal quality units, auditors, health authorities) need to partner with the IT departments and providers to understand the fundamentals before making judgments on

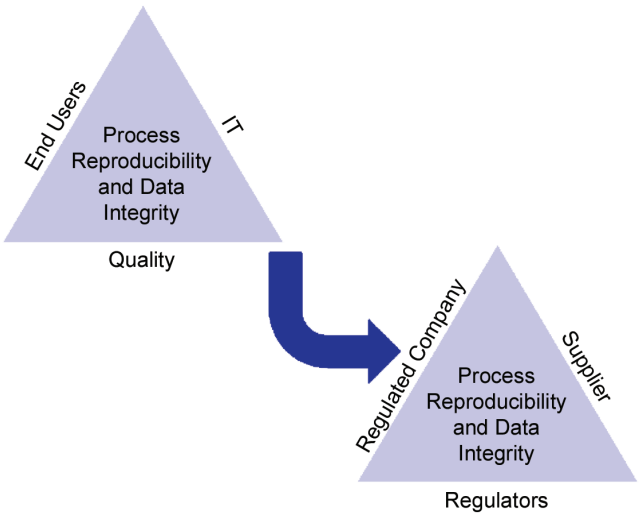

Figure 1. Quality paradigm shift.

the quality of the processes. Quality units need to assess why, where and by whom controls are established and then examine what those controls are. Quality professionals will need to understand the difference between formal elements of control and controls that may impact the data and how this relates to processes being operated at a cloud provider (the difference between what and how). This will likely result in a shift from quality processes contained within a regulated company to a model where quality is achieved as a result of partnership between the regulated company, service providers and regulators - *Figure 1*.

Figure 2 represents a starting point for how one can visualize the partnership that a regulated company and a service provider must prepare. In this arrangement, we must be willing to view controls in a way that they are meaningful, not the same controls moved wholesale to the provider.

As is typical with any change scenario, there will be a certain level of human resistance toward this less proven and unknown territory in which the pharmaceutical companies do not have the control they are used to having. Yet - if we are honest with ourselves – we all know it is the way to go. Think back to the desire to take advantage of advancing technology and avoid paper in the early 90s. The adoption of what we now consider "E-signature" was equally unclear. Industry together with regulators pushed forward and E-signature controls are now embedded into the fabric of regulated companies. So the question in front of us now is about how we can start to better understand and manage (not simply avoid) the risks which come with this technology.

What do we need to do to allow us to:

- Obtain the "promised" cost optimization without compromising the integrity of the data that impacts product quality and patient safety

- Realize the responsiveness the end user demands
- Identify and analyze the risks across and within an enterprise
- Create a framework to manage these risks both in house as well as part of our supplier management processes

The Path to Clarity

In late 2012, and based on an ongoing dialogue between ISPE GAMP Community of Practice (CoP), industry as well as the FDA, it became very clear that there was – and still is – a need to provide guidance on the usage of cloud technologies in the regulated (GxP) environment in order to accelerate adoption of this technology. The GAMP leadership reached out to the FDA, a selection of pharmaceutical companies, and cloud service providers with the request to collaborate on this topic.

The result of this was the formation of a new GAMP Special Interest Group (SIG) in early 2013. A small core team representing a cross section of large and small pharmaceutical companies and cloud service providers SMEs started working together in delivering the guidance to industry and regulators. While the team did not have any idea on the shape or form of this guidance, one thing was clear - the need was high.

The initial questions the team addressed were structured in a simple three-step process:

- What is the current existing guidance for management of computerized systems in a health authority regulated environment?
- What is different in the world of cloud computing? What characteristics force us to look at this differently?
- What is the corresponding framework to combine 1 and 2 into a pragmatic and risk-based approach which satisfies the need of the regulator, regulated company and cloud service provider?

As a starting point, we looked at the following leading industry guidance's:

- The well recognized GAMP® 5 guidance, along with the GAMP® Good Practice Guide on IT Infrastructure Control and Compliance
- The National Institute of Standards and Technology (NIST) Definition of Cloud Computing (Special Publication 800-145)
- The Cloud Security Alliance documents, including the "Cloud Controls Matrix" and "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0"

Once these documents were reviewed and digested, the team focused on the differences between the traditional computer systems and cloud computing services provided by external companies, and how these standards fit with the GAMP® documents listed above. In line with the items already highlighted in this article, the following drivers were identified:

- Shift of controls from the regulated company to the provider
- Presence of regulated companies as a cohesive block in the cloud
- Degree of flexibility and scaling possible

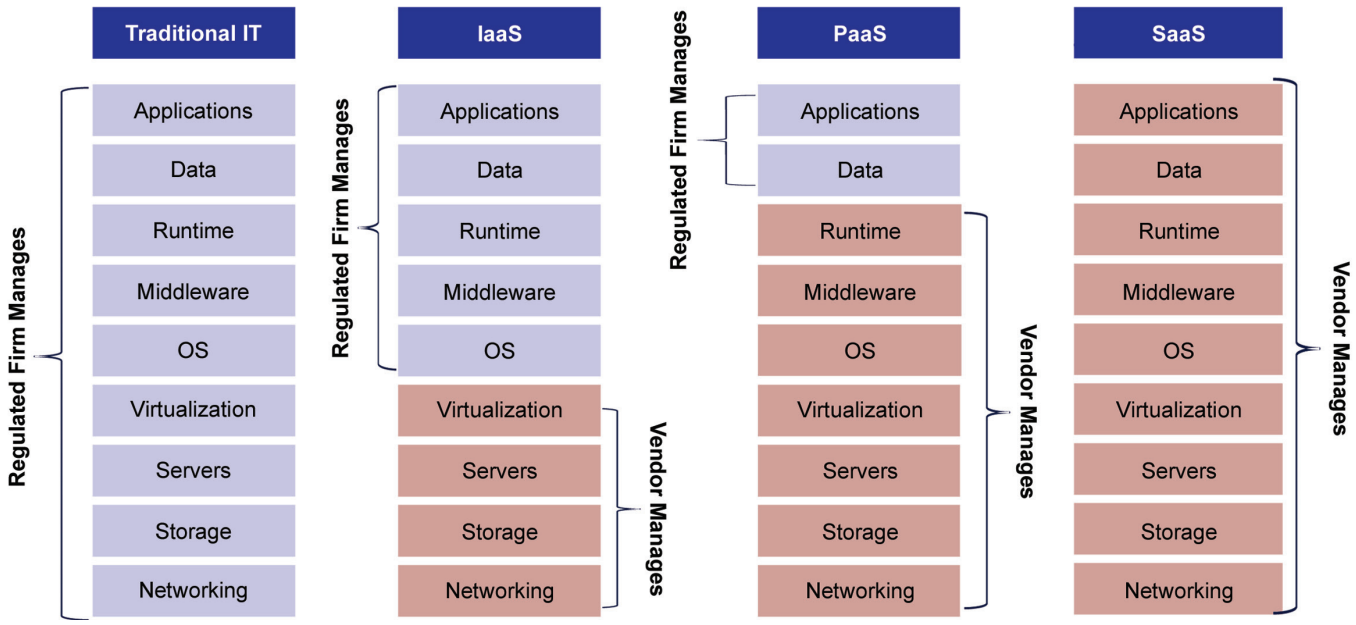

Figure 2. The partnership that a regulated company and a service provider must prepare.

The first difference the group identified is that the use of cloud comes with a never-seen shift of controls across the lifecycle (hardware, applications, or data) from the pharmaceutical companies toward the cloud service provider. Many have seen outsourcing of infrastructure components in the past; occasionally application management is performed by a third party. Many have experienced that each outsourced application support was seen as an almost exotic setup, for which the compliance functions had to initiate intensive discussions with the service provider on how they should manage their application. Our experience has been that there is not even awareness that such transfers of operational activity could raise a compliance concern. Frequently, the individuals involved in such transfers were unaware of the differences and have not engaged a compliance department.

The representation and importance of the pharmaceutical market in a cloud provider's overall customer base is limited.”

The current setup of a Software as a Service (SaaS) looks very much like those abnormal setups on steroids. It involves even greater movement of control toward the supplier, but still leaves the responsibility for the data and process with the regulated company supplier. Infrastructure as a Service (IaaS) on the surface appears like so much less of a compliance risk, but unless tight controls are established to guide what will be stored on top of that infrastructure, compliance concerns are as strong for SaaS. What do those controls look like and when in the lifecycle of information should they be applied? Platform as a Service (PaaS) and the interrelationship of controls between supplier and regulated company is perhaps the most complex. The compliance concerns are just as valid, on infrastructure, platform and even application level, with little or nothing that we as pharmaceutical companies can influence with regard to the providers management processes. Combine this with the fact that many of these cloud service providers are not even willing to open up their companies for audits, and it becomes clear why “cloud” is now one of the most instant “headache triggers” for our traditional quality teams.

Closely linked to the shift of controls, and as already highlighted in the introduction, is the second reason – the fact that the pharmaceutical companies only represent a small market share for the cloud providers, and hence have had little success in telling providers how to run their businesses. Sure, there are exceptions of smaller cloud providers who create an almost on demand setup, but it's no surprise that these are considerably more expensive, and thus less attractive from a pure economical point of view.

Returning to the bigger cloud service providers, it is clear that they do know what they are doing with an excellent track record of uptime and business continuity, and very few security incidents, operating with practices designed for a pure IT industry. There are a wide range of industries already using these services, including the more “conservative” industries such as the banking sector. So why are the processes sufficient for banking and not good enough for large regulated companies? Specialized certifications for companies are possible (CMMI, ISO, etc.). The certifications range from general controls across a provider to area specific certifications such as security. The pharmaceutical industry has occasionally considered a GxP certification for outsourced services, but this thought has never matured. Providers claim to be regulatory ready and some are; however, currently there is no recognized GxP certification process. The SIG is not proposing that one should be developed from new. Existing processes first need to be reviewed objectively to understand the standards and where the differences between the standards and regulated companies expectations may be.

As a first step in mutual understanding, we can look at, for example, ISO 9003:2004 against which GAMP® 5 is aligned. It is a standard that that is frequently accepted as a reference when the pharmaceutical industry audits software providers. Table A demonstrates the fit between GAMP® 5 and ISO 90003 (just one of several controls which also include ISO/IEC 27001:2013 and ITIL®).

Subject	ISO 90003:2004	GAMP® 5, Appendix
Basic Design	7.3.2, 7.3.3	D2/D3
Detailed Design		
Design Review	7.3.4	M5
Code Review	7.3.4, 7.3.5	D4
Module (unit) Test	7.3.6.2 a	D5
Integration/System Test	7.3.6.2 b	D5
IQ/OQ – System Test	7.3.6.2 c 7.5.1.5 7.5.1.6	D5/M7
PQ – Acceptance Test	7.3.6.2 d	D5/M7
Change Control	7.3.7	O6
Configuration Management	7.5.3.2	O6

Table A. The fit between GAMP® 5 and ISO 90003.

As a last difference, we must certainly mention the fact that cloud computing comes with a never before seen level of flexibility and scalability. Along with non-traditional processes for "keeping the lights on" comes the ability to react in minutes and hours to the needs of their customers rather than weeks and sometimes months. Cloud providers can provision space and applications to the end user without the need to assess the impact of such changes on existing systems. Their appeal is that they have what may be considered a narrow range of "products" or "services," but these can be delivered before most regulated companies have finished filling out their change form, not to mention assessing the impacts of those changes.

Clearly, there must be other forces at play. It is not just about the standards. Standards can be aligned. And this is exactly the question that providers are asking us.

A part of the question is answered by recognizing that regulated companies have specific controls that cover all of the classic software development standards and which are stricter than what we have seen in other industries. There are expectations of performing in-depth impact assessments toward product quality and patient safety when changes are made to any system. There is an expectation that during the development and operation of a system, a quality/validation "plan" is established to assure a system is delivered fit for use and can be maintained as well. Lastly, there is an expectation that the performance of activities, such as development, testing, release, etc., be formally documented. The expectation is that the process and the outcomes are reviewed, approved and preserved for future examination. The fact that we have historically executed some operational controls in a "different" way is not a good reason for not adopting innovative approaches, as long as quality, integrity and compliance are preserved.

The First Steps on Our Journey

The fact that these processes in the cloud are different does not mean that they are inferior. It is up to the pharmaceutical industry to analyze these differences, identify resulting gaps, and manage the corresponding risks. The first step in this journey is to recognize the different cloud deployment models, the traditional IT controls and underlying actions, to understand who needs to execute the controls. To do so, controls, such as ISO/IEC 27001:2013, ITIL®, European Network and Information Security Agency (ENISA) also should be considered. If we are to operate in a new paradigm, we must look beyond the current practices of the pharmaceutical industry.

This first exercise will provide the SIG with a clear and detailed overview of the responsibilities between the cloud service provider and the regulated company. These traditional controls will have to be accounted for within a company's quality framework, and then we must step back in order to understand if this new model will require different or additional controls to ratify the rigor of the regulated industry.

Once this analysis is completed, the SIG will examine supplier management controls and how they may need to be re-considered. Additionally, we will further examine which IT controls are best performed by the service provider, as well as current certification programs commonly attained by providers. Only then with this analysis and dialogue between cloud providers, regulated companies and regulators can a framework be created that will satisfy the regulated industry.

The Future – What's Coming

In the coming months, the SIG will examine the ways in which the pharmaceutical industry is or would like to use the different services (IaaS, PaaS, SaaS), GAMP® vs. IT standard controls and providing recommendations on how to assess the risks, identify gaps and provide recommendations for the changing landscape of regulated IT controls.