SaaS in a Regulated Environment – The Impact of Multi-tenancy and Subcontracting

July 2016

A Concept Paper by the ISPE GAMP Community of Practice

Acknowledgements

This Concept Paper was written and reviewed by members of the GAMP® Cloud Special Interest Group (SIG) of the ISPE GAMP® Community of Practice (COP). It represents industry best practices based on the experiences and input from the individuals listed below and does not reflect the views of any one individual or company.

SIG Chair

Kathy Gniecko	F. Hoffmann-La Roche	Switzerland

SIG Sponsor

Michael Rutherford	Eli Lilly and Company	USA

Document Authors

Ekaterina Sidorova	Novartis Pharmaceuticals	Switzerland
Phil Harrison	Formpipe Life Science	United Kingdom

Particular thanks go to the following for their support of this Concept Paper:

Chris Clark	TenTenTen Consulting Ltd.	United Kingdom
Arthur (Randy) Perez	Novartis Pharmaceuticals	USA
Sion Wyn	Conformity Ltd.	United Kingdom
Christopher White	Alexion	USA

Table of Contents

In two articles published in *Pharmaceutical Engineering* [1] and [2], the GAMP® Cloud SIG provided an overview of some of the primary challenges and concerns regarding whether cloud solutions can be adopted, as well as the specific challenges related to the Infrastructure as a Service (IaaS) delivery model.

The GAMP® Cloud SIG has now created three companion Concept Papers covering the topic of Software as a Service (SaaS) and Platform as a Service (PaaS):

- "SaaS in a Regulated Environment – The Impact of Multi-tenancy and Subcontracting" (this Concept Paper) is focused on the SaaS cloud model description, various business models used by the SaaS providers and security and privacy concerns related to those models.

- "Using SaaS in a Regulated Environment – A Life Cycle Approach to Risk Management", looks into the life cycle of the relationship between regulated company and SaaS provider and delves deeper into the issues a delivery team can face in their exploration of moving a business supporting system to a SaaS provider.

- "Evolution of the Cloud: A Risk-Based Perspective on Leveraging PaaS within a Regulated Life Sciences Company" is intended to help to explain how PaaS compares to other cloud solutions (specifically IaaS), as well as discussing risks and associated pragmatic controls that regulated companies should consider when leveraging PaaS within their organization.

1 Introduction

In the evolving regulated IT environment there are many things to consider when thinking of turning to the cloud for a solution. Using a SaaS provider can be an excellent option, but doing appropriate research and establishing the company's specific needs are critical to making the right decision when having so many choices of providers, models and risks associated with each. This Concept Paper attempts to provide an overview into some of the current thinking on this topic in relation to the SaaS model.

SaaS risks should be weighed against the benefits of the IT solution's lower ownership costs, as well as an optimized infrastructure. The latter allows for quick access to those computing services which are increasingly important in order to effectively process the volume of data produced in an increasingly computer dependent industry.

This Concept Paper considers some of the various models of SaaS being offered today along with issues and risks to consider when selecting a reliable, secure, and economically sound provider. In particular, it highlights the differences that subcontracting and multi-tenancy can bring, when compared to basic, private SaaS offerings. It also considers how key areas of security and privacy may be affected by these different models.

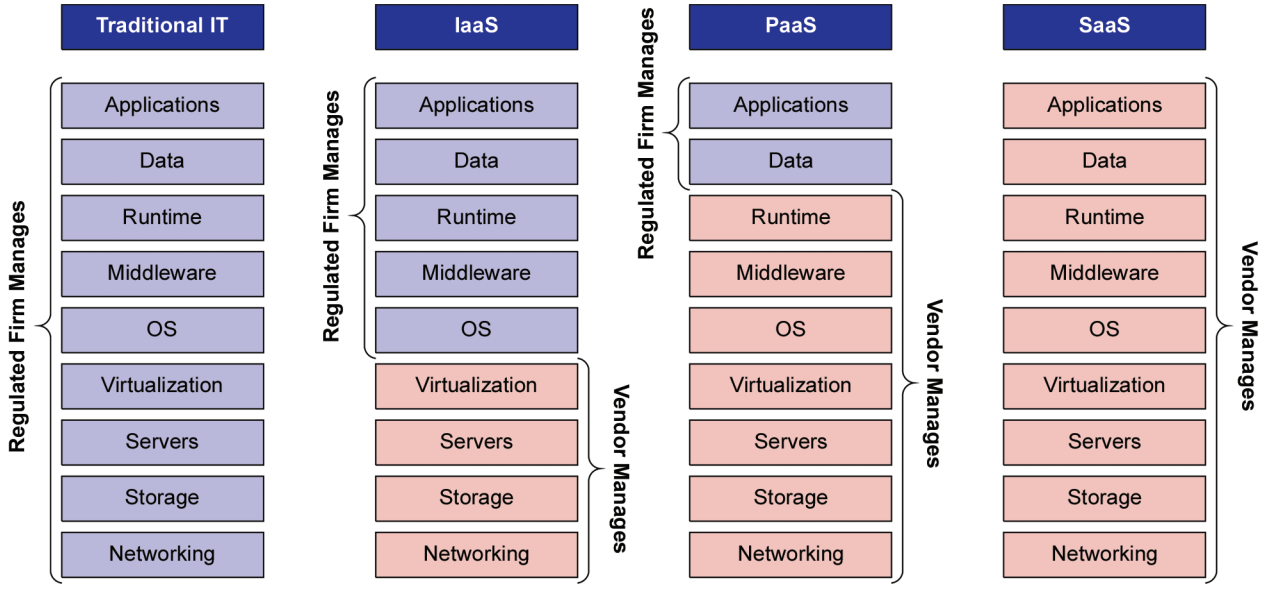
These considerations should allow further investigation of the subject while armed with some important background information, together with an understanding of the risks and decision points when planning a move to a SaaS offering.

The model appropriate for a regulated company's particular needs with a provider offering reliable, quality, robust services with minimal risk is a basic set of requirements for any industry, but is particularly important for regulated pharmaceutical and biopharmaceutical companies.

2 Scope

In the introductory article “Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity” [1] an overview was provided of some of the primary challenges and concerns which were debated by the regulated industry regarding whether or not cloud solutions could be adopted. In that article the following model was introduced to provide a framework of computer system components and where the control for the components reside. A second article produced by the GAMP® Cloud SIG [2] explored the challenges of adopting the Infrastructure as a Service (IaaS) delivery model within the regulated environment.

Figure 2.1: The Elements of Partnership That Should Be Prepared for with a Service Provider



This Concept Paper explores Software as a Service (SaaS) delivery models currently offered and will highlight the impact of subcontracting and multi-tenancy on SaaS arrangements. These two dimensions can make a significant difference to the risks associated with SaaS, in particular with the key areas of Information Security and Data Privacy.

The Concept Paper focuses on the data maintained at a SaaS provider.

3 The SaaS Model

The widely accepted definition of Software as a Service model by National Institute of Standards and Technology (NIST) is:

> *"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings".*

The NIST SaaS Model can appeal to regulated companies and their IT departments by signifying the potential for:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

For the end users, some of the detail of cloud characteristics or the risks associated with the deployment model may be not be immediately apparent from this definition. The key concern for regulated businesses as users of SaaS applications, is that another organization is in control of:

1. The infrastructure on which the business's data resides
2. The software and data belonging to the business

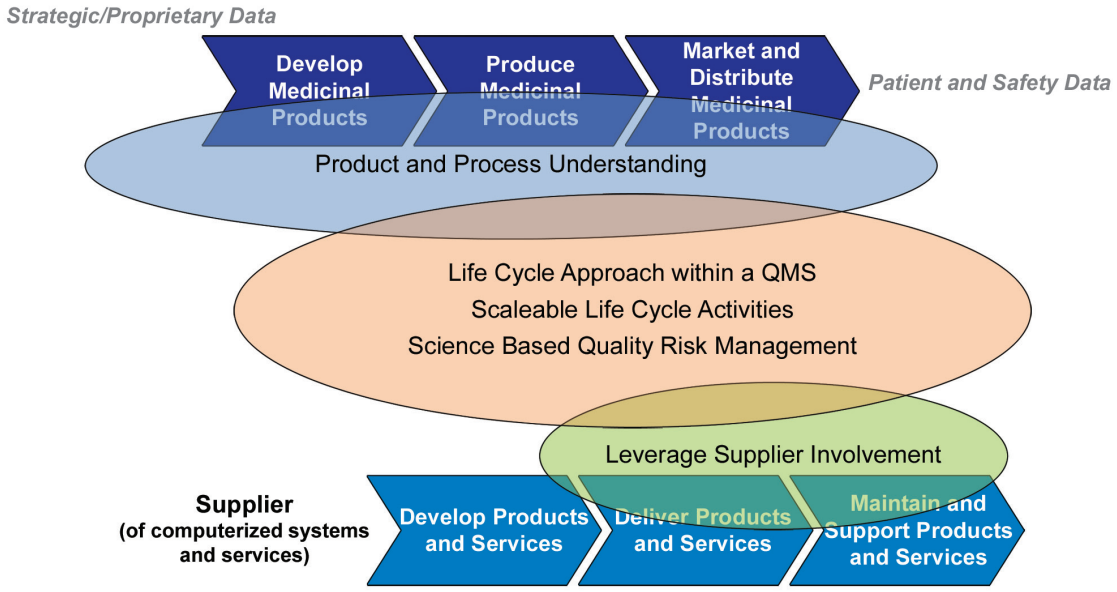
All SaaS solutions will share this common concern, but differences in the underlying cloud infrastructure characteristics and deployment models by each provider means that different SaaS solutions need to be handled in different ways.

4 Considerations When Moving to a SaaS Arrangement

The decision to move from an internally hosted software application model to a SaaS model should be made with an understanding of the full context of business processes and the data generated during the execution of those business processes.

GAMP® 5 introduced a model (Figure 4.1) that can help to visualize the elements of pharmaceutical processes and data potentially "at risk" by hasty or not well thought out movement to a SaaS provider.

Figure 4.1: Risk Areas for Pharmaceutical Process Outsourcing



The concerns for SaaS solutions set up to support business activities early in the "value chain", i.e., research and early development, will be different to those when solutions are used to support business processes with direct and immediate implications on patient and product safety.

The sensitivity of the data to be housed in the SaaS solution needs to be at the heart of any decision about the SaaS provider, e.g.:

- As the project evolves through its life cycle, then controls established to protect intellectual property data needs to keep pace with the information to match the progression into the GxP supporting data that may impact patients and product. This progression will include more than data security controls. It needs to support, via the demonstrable strength of the security and privacy controls, that integrity of the data across the entire life cycle of the data can be maintained.

- When data directly impacts the patient, more traditional GxP controls (e.g., training records, independent oversight of changes) become more important in demonstrating control of the application.

When choices are available, preference should be given to providers that can demonstrate a closer understanding of how an IT company and its controls integrate with the ability to provide safe and effective pharmaceutical product.

5 Different SaaS Models

Figure 5.1: Possible Infrastructure Models for a SaaS solution

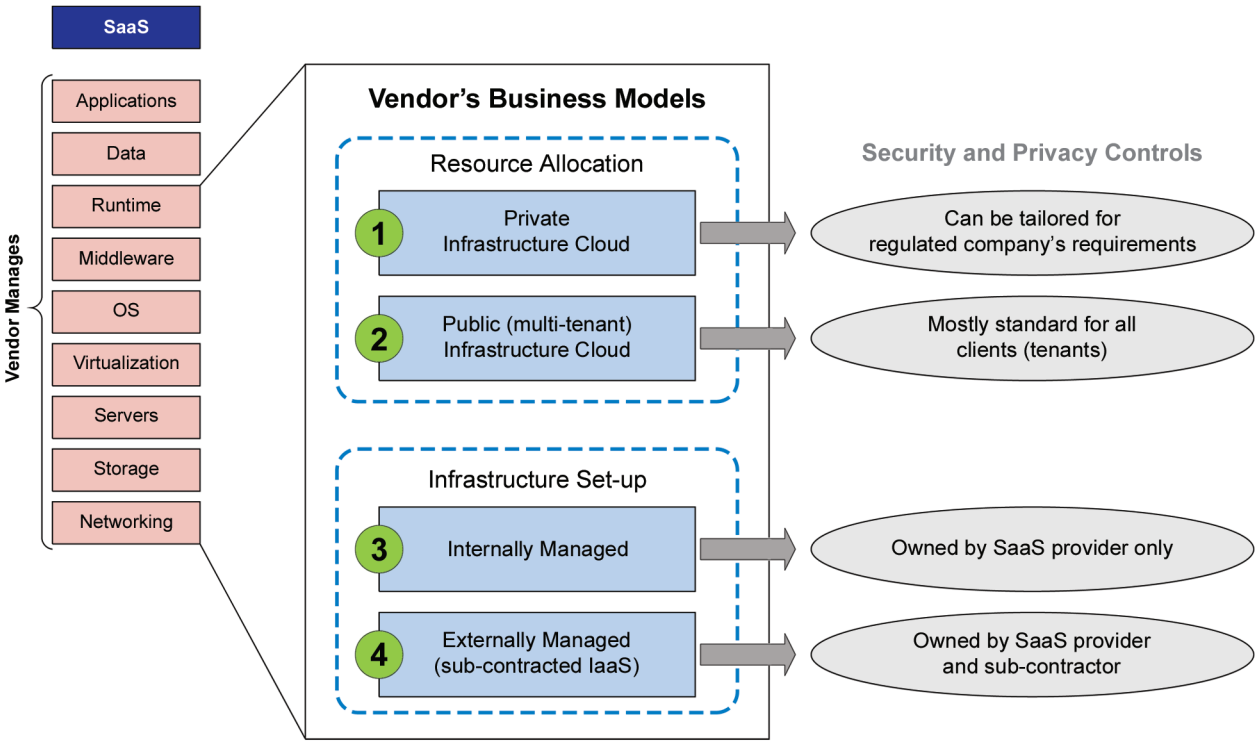


Figure 5.1 represents the possible configuration scenarios of private/public and internally/externally managed infrastructure models that will support the SaaS provider offerings. Depending on how the computer resources are allocated, the infrastructure for a SaaS solution can be:

- Dedicated to one customer (i.e., private cloud infrastructure model)
- Shared by multiple customers (i.e., public cloud infrastructure model)

For simplicity, intermediate models, such as community or hybrid cloud infrastructure models, are considered versions of the public cloud.

Based on the Infrastructure setup the following models can be defined:

1. SaaS solutions based on the private cloud infrastructure (Green Circle 1)
2. SaaS solutions with multi-tenant architecture (Green Circle 2)
3. SaaS providers that directly manage the infrastructure of the application (Green Circle 3)
4. Where infrastructure is managed externally by third party Infrastructure as a Service (IaaS) provider (Green Circle 4)

SaaS solutions based on the private cloud infrastructure (Green Circle 1) are similar to using an internal IT department. When the infrastructure is fully dedicated to the SaaS solution for only a single regulated company, this offering is effectively a traditional outsourcing model. Regulated companies can have a significant influence over the SaaS providers which utilize this model.

To achieve more cost reductions and computer resources scalability many regulated companies are considering SaaS solutions with multi-tenant architecture (Green Circle 2). In these situations, an individual regulated company may have much less influence over the SaaS provider. This is a public SaaS set-up, frequently with standard service levels available to all clients (including those belonging to non-regulated industries). Although such SaaS solutions may allow specific configuration settings, this is not always the case.

Management of the infrastructure can also be divided into two offerings, managed internally by the SaaS provider (Circle 3), or externally by a separate IaaS provider (Circle 4). As with circle 1, this arrangement is close to a standard outsourced scenario, offering the possibility that the regulated company can negotiate and pay for additional controls deemed necessary.

In cases where the SaaS provider sub-contracts aspects of its infrastructure management to a third party on an IaaS basis (Green Circle 4) the risk is that the regulated company has even less control, but continues to bear full accountability over its security and compliance. This model is relatively common in situations where the SaaS provider is familiar with regulated industry requirements, but is using a partner with extensive datacenter facilities to provide a colocation service using dedicated (private) equipment. In such cases it is important for the regulated company to determine exactly which services the sub-contractor is providing, and to ensure that the subcontractor has been, or will be, appropriately assessed.

There can be a range of states between these various SaaS models. When assessing which suppliers to use, and how to use them, both multi-tenancy and subcontracting should be considered.

The SaaS provider may also subcontract infrastructure services to another company that is using a public cloud infrastructure; therefore, combining the risks that multi-tenancy and the use of sub-contractors may introduce. This option can be relatively common, as a result of seeking economies of scale and pricing.

The concept of “multi-tenancy”, based on a public cloud infrastructure within the SaaS delivery model, presents risks that are likely to become key issues for regulated companies. It is usually the most attractive option from a costing and responsiveness perspective, but it is also where regulated companies have the least control over the solution delivery.

In order to take advantage of cloud computing capabilities, adequate quality controls should be established, that take into consideration the:

1. SaaS solution selected by the regulated company

2. SaaS provider

3. SaaS provider’s sub-contractors

6 Data Security and Privacy

Data security and privacy are usually of greatest concern when moving fully to a SaaS provider (i.e., a multi-tenancy SaaS solution).

6.1 Security

The issue of trust in the SaaS solution provider's security controls is a consideration in all SaaS models, because control over security operations is primarily in the hands of the SaaS provider. For multi-tenancy SaaS arrangements (see Figure 5.1 (Green Circle 2)), however, there are several aspects of security that should be considered specifically.

Where a SaaS provider has better security controls than a regulated company, putting trust in that provider may be fully justified.

However, multi-tenancy or shared access to the servers where data resides can also be perceived as having a greater potential to opening the doors to hackers, since the provider may be a more attractive target based on the other tenants hosted by a provider.

In addition, authentication, authorization and sometimes even access control is now handled by someone who needs to have awareness of the requirements of the processes the SaaS solution will support, which is significantly more complex in a multi-tenancy solution. This has a greater potential for compromising data in the segment of those servers used by the regulated company.

The GAMP® Cloud SIG article "Challenges for Regulated Life Sciences Companies within the IaaS Cloud" [2] identified the training of IaaS providers as a strong consideration for this particular reason.

For SaaS arrangements that include an IaaS sub-contractor (see Figure 5.1 (Green Circle 4)), the complexity is further increased by adding new players and steps to the security process, e.g., for breach reporting. A possible mitigation measure is to clarify communications and response times for Breach notification through Service Level Agreements (SLAs) or Quality Agreements (QAGs). A process should be implemented to ensure that notifications to the regulated company occur, as there is no direct contact between regulated company and the sub-contractor.

In addition, personnel of both the SaaS provider and its subcontractors should be aware of the of the importance of the data they hold. This, combined with robust security controls, is key to establishing a foundation which increases assurance of the integrity of the regulated company's data.

When dealing with a multi-tenancy environment, a flaw could allow another tenant or attacker to see restricted data or to fraudulently assume the identity of individuals. Depending on what business processes are supported at a SaaS provider, potential risks like these should be considered before entering into a relationship with the provider.

6.2 Privacy

When personal data, i.e., information that can be related to an identifiable person, is likely to be processed within the SaaS solution, the matter of compliance with the applicable data privacy laws and regulations should be considered. It can be argued that subcontracting the IaaS element of the SaaS arrangements (see Figure 2 (Green Circle 4)) increases the potential risks with respect to Privacy.

The number of privacy regulations world-wide is considerable , yet many have in common data protection principles, first introduced in the Organisation for Economic Co-operation and Development's (OECD) "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" in 1980 and expanded in the UK's Data Protection Act, EU Data Protection Directive (Directive 95/46/EC) [3], EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [4], Privacy Shield [5], etc. The following principles should be considered when engaging the SaaS provider:

- **Data is obtained only for specified and lawful purposes.** Where applicable data subjects (individuals) have to be informed that their data will be processed by the SaaS provider and all its sub-contractors (legal entities and/or locations)

- **Data accuracy and integrity ensured.** Regulated companies should define the process allowing data subjects to request changes to their data. In the case of use of sub-contractors, the regulated company should ensure that a SaaS provider will ensure that the respective process is in place with each sub-contractor used.

- **Data not stored longer than necessary.** A regulated company should have established the retention periods of the personal data and should clarify the roles and responsibilities in case of destruction of data stored at a SaaS provider. In the case of sub-contractors, the SaaS provider has to ensure that the respective process is in place with each sub-contractor.

- **Transfer only to countries with adequate protection.** The responsibility rests with the regulated company to know the SaaS provider's location, and the locations from which data will be accessed. This includes access by SaaS provider's associates, as well as where the data will be physically hosted. The regulated company needs to ensure that all these locations can provide the required level of data protection (through audits, Data Transfer Agreements, etc.).

7 References

1. ISPE GAMP® Cloud Computing SIG, "Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity," *Pharmaceutical Engineering*, Jan/Feb 2014, pp. 58-62, www.pharmaceuticalengineering.org.

2. Streit, Robert and Anders Vidstrup (Members of the ISPE GAMP® Cloud Computing SIG), "Challenges for Regulated Life Sciences Companies within the IaaS Cloud," *Pharmaceutical Engineering,* Sept/Oct 2014, pp. 72-82, www.pharmaceuticalengineering.org.

3. Directive 95/46/EC, EU Directive on the Protection of Personal Data, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

5. EU-US Privacy Shield – Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC," http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf.

8 Acronyms

GxP	Good X Practice (X can mean: Clinical, Laboratory, Manufacturing, Pharmaceutical, etc.)
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
QAG	Quality Agreements
SaaS	Software as a Service
SIG	Special Interest Group
SLA	Service Level Agreement

ISPE®

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org