Evolution of the Cloud: A Risk-Based Perspective on Leveraging PaaS within a Regulated Life Sciences Company

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) 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

Michael Crowthers	Deloitte & Touche LLP	USA
John Conrad	Deloitte & Touche LLP	USA

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

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

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" 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" (this Concept Paper) 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

Over the past decade, the life sciences industry has seen cloud-based services and solutions evolve from a misunderstood technology that few regulated companies were comfortable using, to a mainstay solution adopted by many seeking to capitalize on numerous value propositions highlighted by cloud providers. These benefits include the ability to drive business innovation fueled by the speed at which a cloud solution can be made available or "spun up", as well as the ability of the IT function to reduce overall costs and overhead, by leveraging a variable cost model rather than managing fixed costs of in-house IT solutions.

The evolution of cloud-based services and solutions in the Life Sciences industry can, in part, be attributed to the focus many leading cloud providers place on security and data integrity. In addition, many leading cloud-based providers are developing teams which are focused on the life sciences industry. These teams include members who understand the regulated nature of the life sciences industry and are focused on developing approaches, processes, and controls to address regulatory requirements.

Although there has been progress in understanding the controls required by both the regulated companies and the cloud providers, there are still some questions that remain unanswered. This is especially true for Platform as a Service (PaaS).

Many regulated companies continue to struggle with PaaS by attempting to apply existing policies surrounding the System Development Life Cycle (SDLC) or security-to-PaaS solutions. Those policies were originally intended to address traditional on-site systems where the regulated company had control over the entire technology stack from hardware up to the software layer. Control now is divided between cloud provider and cloud customer.

In a previously published article, "Challenges for Regulated Life Sciences Companies within the IaaS Cloud" [2], the focus was on the key items that need to be addressed to adopt an IaaS model within a regulated organization.

As a continuation of the series, this Concept Paper will help 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.

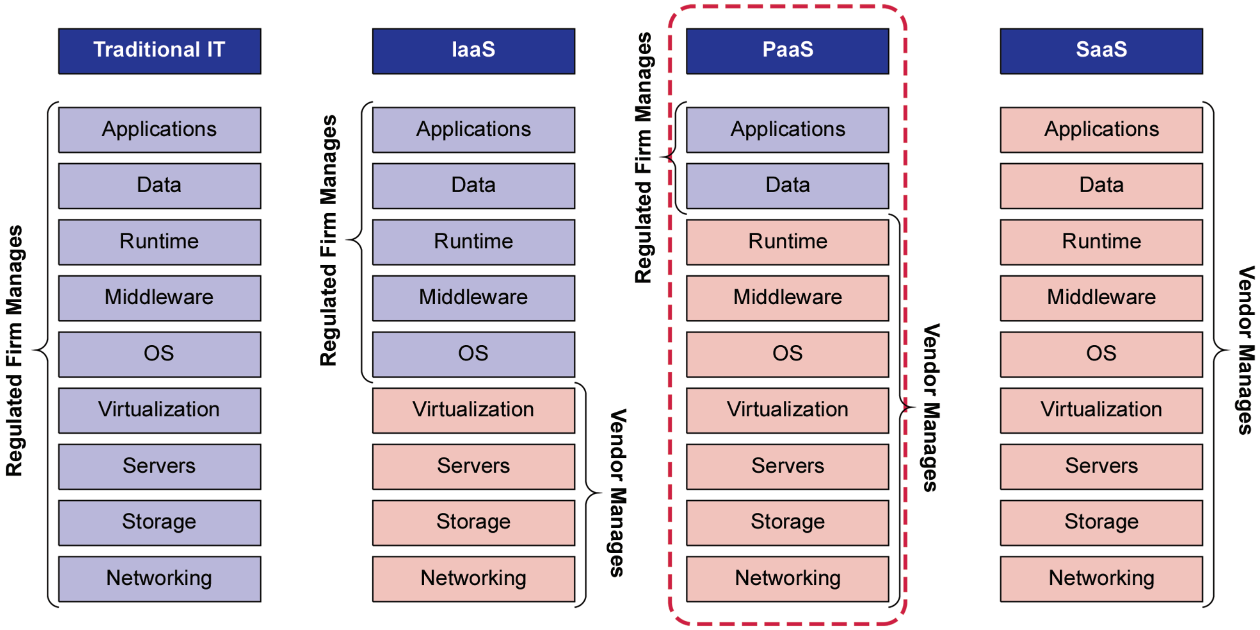
2 Defining the PaaS Difference

NIST defines PaaS as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider [3].

The purpose of PaaS is to provide a programming platform to create a software application solution without the overhead of hosting and maintaining the underlying technology stack.

While the regulated company is ultimately accountable for ensuring that systems are fit for use, Figure 2.1 shows where other lines of ***responsibilities*** can be drawn for PaaS between cloud providers/vendors and cloud customers/regulated companies (see Figure 2.1).

Figure 2.1: Regulated Company and Vendor Responsibilities Across Cloud Services



2.1 Rising Use Cases for PaaS

General use cases for PaaS are increasing and are cutting across the entire life sciences value chain Some examples are listed in Table 2.1.

Table 2.1: Example PaaS Use Cases Across Industry Domain
Used with permission from Deloitte Development LLC, www.deloitte.com. Copyright © 2016 Deloitte Development LLC. All rights reserved.

Industry Domain	Example Solutions
Commercial	• Contact/Call Center and Medical Information • Sample Disbursement • Service Management • Patient and Health Care Provider (HCP) Portals • Brand and Disease State Portals • Speaker Program and Events Management • Key Opinion Leader (KOL) Management • Order Management/Rebate and Contract Pricing
Research and Development	• Investigator Collatoraion • Patient Recruitment • Business Development • Product Launch Management • Content Management • Clinical Data Management
General and Administrative	• Employee, Partner, and Field Collaboration • Service/HR Help Desk • HR Performance Management
Quality and Compliance	• Corrective and Preventative Actions (CAPA) Management • Complaint Management • Content Management • electronic Trail Master File (eTMF) • Compliance Operations • Training
Pharmacovigilance	• Risk Evaluation and Mitigation Strategies (REMS) Programs • Adverse Event Management
Supply Chain and Manufacuring	• Third Party Intermediaries Management • Partner Relationship Management • Contract Manufacturing Organization (CMO) Forecasting • Unique Device Identification (UDI)

3 Gauging the Pressure of PaaS Risks

Life Sciences companies should be aware that cloud computing introduces several challenges (i.e., risks) including:

- Legal and Compliance
- Security and Data Privacy
- Data Integrity
- Business Continuity

This Concept Paper discusses these risk areas in the context of how they relate to a PaaS platform.

3.1 Legal and Compliance Risk

PaaS solutions are unlikely to address regulatory compliance risks based on out of the box native functionality. For example, when considering regulations such as 21 CFR Part 11 (Electronic Records; Electronic Signatures) [4], the regulatory requirements, such as electronic signature controls or system generated time stamped audit trails, appear challenging for many PaaS providers to address without:

- some level of solution customization at the application layer
- the need for a bolt on tool
- enhancement to existing processes

The time and ability to implement these controls should be considered early in the selection of the provider. While each can be achieved, the level of complexity increases if a chosen PaaS provider requires electronic signatures. This would require further considerations surrounding the authentication of users, as well as the effects of vendor changes on custom built signature functionality.

In addition, the ability for PaaS providers proactively to demonstrate compliance with system change management controls is a significant challenge.

Change management is necessary from two perspectives:

1. Changes to the technology stack for the platform can have an indirect impact on data integrity, and in some cases may have an immediate and direct impact:
    - The PaaS vendor should have a process established to evaluate changes and to properly communicate changes to customers.
2. As a user of PaaS, the regulated company needs to assess the impact of the changes to their application supported by the underlying platform. While changes to the underlying platform may not appear to be a risk, in some cases the change could have an unintended impact on the application layer, e.g.:
    - an upgrade to the operating system could cause compatibility issues with a specially designed application. This could affect how data is recorded through the application, or in some cases make the application inoperable. Potential risks to data integrity can be mitigated by establishing processes to assess and track these changes.

3.2 Security and Data Privacy Risks

When using a PaaS platform, the regulated company may manage controls which reside in the front-end application, e.g.:

- Data asset classification
- System access
- Identity management

The PaaS platform is typically under the control of the PaaS provider and, therefore, source code/platform data security and privacy risks are also managed by the PaaS provider. For example, many PaaS data architectures are public clouds and are multi-tenancy. The cloud provider is responsible for the initial design and implementation of security and data protection controls, as well as the ongoing administration of those controls on the platform components for *all* tenants on the platform.

In order to address these data security risks, regulated companies should consider the data asset classification of data that will flow through the PaaS platform. This will help in determining regulatory and/or legal implications associated with that data. This risk classification can assist in identifying the types of security controls that should be considered as part of a PaaS provider selection and management process. Some of the security controls to be considered include:

- Encryption levels on data (both in storage and transfer)
- Vulnerability scans
- Identity and Access Management policies and procedures
- Security Incident Management process

3.3 Business Continuity and Data Integrity Risk

Another common set of risks related to PaaS technology is the availability, reliability, and recovery of data hosted on the cloud platform. In order to assess a provider's capabilities, the regulated company should define its business continuity requirements. This information should drive the application-specific recovery needs. The continuity plan should take into account considerations around recovery target, potential data loss risk, and the lag time for failover and service restoration in order to reduce the impact to business operations, as well as data integrity.

Once the business continuity planning requirements are understood, there are several key capabilities to consider when reviewing a PaaS provider's disaster recovery processes and infrastructure; these include:

- Procedural controls and training
- Failover site location
- Frequency of backups
- Failover periodic testing
- Failover lag time
- Communication plan (internal and external)

As part of an evaluation of how PaaS vendors address these disaster recovery controls, consideration should be given to mapping their capabilities to business continuity requirements and/or an established Business Continuity Plan. How factors such as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) will be met should also be considered.

4 Qualification and Validation Considerations Surrounding the PaaS Platform

Qualification and validation of PaaS requires clear delineation of responsibilities of the PaaS vendor as compared to the regulated company that uses their services.

Qualification (or Verification) of the PaaS platform is the responsibility of the PaaS provider. The qualification process and maintenance of changes and supporting qualification records should be reviewed as part of the vendor audit process. While the qualification activities are the responsibility of the provider, it is the responsibility of the customer/regulated company to determine that their provider has the proper controls in place.

At a minimum, the PaaS provider audit should include a review of:

- System Development Life Cycle (SDLC) and supporting procedures – as it applies to the platform
- Qualification process and/or protocol
- Release management process
- Change management process
- Security
- Data Center Environmental/Facilities management
- Training processes

Table 4.1 provides an example of how the IT audit considerations of the cloud services provider can be additive through the various cloud layers from IaaS through SaaS.

Table 4.1: Example IT Audit Considerations Through the Cloud Service Layers

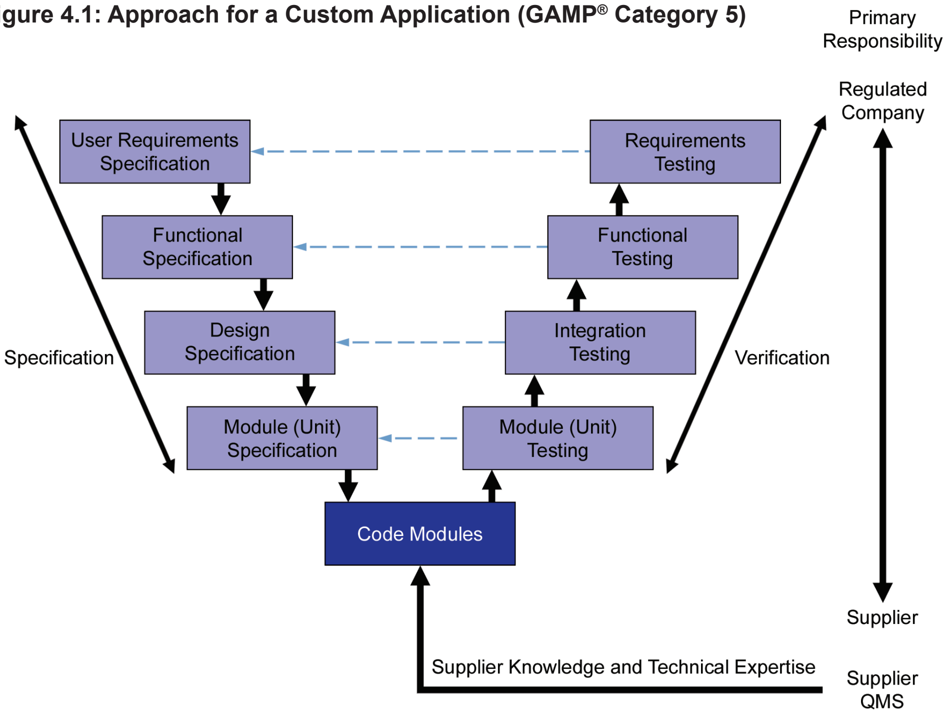
Used with permission from Deloitte Development LLC, www.deloitte.com. Copyright © 2016 Deloitte Development LLC. All rights reserved.

Service Type	IT Quality Management System	Infrastructure Qualification	Security and Privacy
SaaS	• Software Quality Assurance Program • SDLC • Computerized System Validation • Electronic Records and Electronic Signatures • Archiving • Records Management	• Application	• Identity and Access Management • Policies and Patching • Cyber Alerting and Monitoring • Testing Strategy and Approach • Virtualization Architecture • Privacy and Legal Requirements • Incident Response • Access Controls • Vulnerability Management • Logical and Physical Controls • Data Ownership • Disaster Recovery • Availability and Reliability
PaaS	+ SDLC • Patch Management • Release Management • Data Migration	• Applications • Libraries • Tools	
IaaS	+ Change Control • Configuration Management Database (CMDB) • Provisioning • Incident and Problem Management • Disaster Recovery • GxP Training	• Servers • Storage • Virtual Management Software	

Conversely, ***Validation***, in the context of this Concept Paper, relates to the validation of custom applications developed by the regulated company that are hosted on the cloud platform. These validation activities and the related documentation are the responsibility of the regulated company to create and maintain.

The application should be validated as GAMP® Category 5 software, as recommended by GAMP® 5 [5], see Figure 4.1.

Figure 4.1: Approach for a Custom Application (GAMP® Category 5)



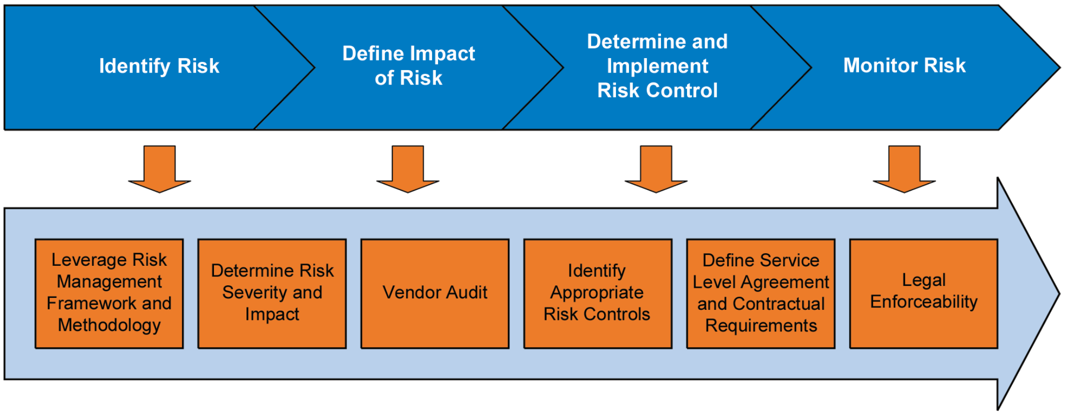
5 Applying a Practical, Risk-Based Approach as well as an Integrated Framework

Before making the decision to adopt PaaS to enable GxP regulated processes and data, the level of acceptable risk for each of the sample risk areas discussed, as well as the capability to manage those risks, should be evaluated and understood. This should confirm the confidentiality, integrity, and availability of data.

This can be achieved via the development of:

1. A risk-based cloud adoption strategy and associated methodology, e.g., the process outlined in Figure 5.1.

Figure 5.1
Used with permission from Deloitte Development LLC, www.deloitte.com. Copyright © 2016 Deloitte Development LLC. All rights reserved.


Identify Risk
Define Impact of Risk
Determine and Implement Risk Control
Monitor Risk
Leverage Risk Management Framework and Methodology
Determine Risk Severity and Impact
Vendor Audit
Identify Appropriate Risk Controls
Define Service Level Agreement and Contractual Requirements
Legal Enforceability

2. An integrated cloud risk management process that provides the following benefits:

   - Provides a broad compliance program versus managing compliance against individual regulations and requirements
   - Incorporates existing GxP, IT, business and security regulations, standards, and frameworks
   - Rationalizes duplicate and inconsistent requirements
   - Provides a common definition of controls and detailed implementation requirements
   - Organizations can demonstrate compliance to a variety of regulated entities

6 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. NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, National Institute of Standards and Technology (NIST), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

4. 21 CFR Part 11 – Electronic Records; Electronic Signatures, Code of Federal Regulations, US Food and Drug Administration (FDA), www.fda.gov.

5. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, www.ispe.org/guidance-documents.

7 Acronyms

GxP	Good X Practice (X can mean: Clinical, Laboratory, Manufacturing, Pharmaceutical, etc.)
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SDLC	System Development Life Cycle
SIG	Special Interest Group

ISPE®

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

www.ISPE.org