



Cloud Framework, Pre-Amble

Contents

1	Executive Summary.....	1
2	Background and Acknowledgements	1
3	Cloud Services – An Introduction	2
3.1	Cloud Service Models vs. Traditional Computerized System.....	2
3.1.1	GxP Computerized System Context	2
3.1.2	Cloud Service Models.....	3
3.1.2.1	Infrastructure as a Service (IaaS).....	4
3.1.2.2	Platform as a Service (PaaS)	4
3.1.2.3	Software as a Service (SaaS)	4
3.2	IT Supply Chain in the Cloud Era	4
3.2.1	Cloud Roles	4
3.2.2	Activities and Examples in the Cloud Supply Chain	4
3.2.2.1	Examples of Scenarios	4
3.2.2.2	Examples by Role	5
4	GxP Considerations for Cloud Service Customers and Cloud Service Brokers.....	7
4.1	SDLC Policy - Cloud Specific Guidance.....	8
4.1.1	Supplier Management Policies	9
4.1.1.1	Quality Agreement Considerations	10
4.1.2	Information Risk Management, Privacy and Data Protection Policies.....	11
4.1.3	Cyber Security	12
4.2	Continuous Delivery and Continuous Validation.....	13
4.2.1	The Challenge.....	13
4.2.2	The Approach	14
4.2.3	DevOps.....	14
4.2.3.1	Configuration Management	14
4.2.3.2	Change Management.....	15
5	Glossary	16
6	References.....	17

Revision History

Version	Date	Summary
WP-23	2023-OCT-13	<ul style="list-style-type: none">• Minor update of section 1 to reflect paper.• Minor change to chapter 2 to reflect the purpose of the working group.• Second question in section 3.1.2 updated partly.• Table in section 3.2.2.2. restructured and updated.• New section 4,2 including subsections.



Cloud Services

A Framework for Adoption in the Regulated Life Sciences Industry

Pre-Amble

Last Update: 2023-06-22

This document has been developed by the Pharmaceutical User Software Exchange (PHUSE) Working Group on Cloud Adoption and is subject to ongoing consultation and feedback from all relevant stakeholders.

You may submit comments and suggestions regarding this document to avid@nnit.com (Anders Vidstrup, NNIT A/S).

**Pharmaceutical User Software Exchange
Cloud Adoption Working Group**

1. Executive Summary

In adopting cloud-based solutions for GxP workloads, understanding the essential characteristics of cloud services and solutions is important for determining the applicability of GxP requirements to specific Cloud Service Providers and/or cloud-based solution models.

At a superficial level, this framework describes Cloud Service models and their relationships to “traditional GxP Computerized Systems”.

When adopting cloud services for GxP uses, Cloud Service Customers, Cloud Service Brokers and Cloud Service Providers should review and evaluate three major control areas within their organization (but not limited to):

- Organization policies and standards
- System-level controls
- Supplier and Vendor Management.

Since the original publication of this framework, adoption of the public cloud by Life Sciences has become necessary, and no longer the exception. As part of this foreseeable evolution, there has been a significant rise in the construction of hybrid and/or multi-cloud systems. One of the drivers of this transformation is the rapid rise of Intelligent Automation driving a) leverage of cloud services enabling ML/AI development and b) the need to ingest data from multiple data sources for model development. With that said, Cloud services leverage many existing technologies and, consequently, there are many ways in which the development and validation of GxP computerized systems built with cloud services may be achieved.

It is also the case with cloud services that “the sum of the parts is greater than the whole”, and that system development and validation activities take on many new and beneficial characteristics that are commensurate with the generic characteristics and benefits of cloud services generally. This framework outlines these approaches leveraging well-recognized concepts. Topics such as Governance and Supplier Management and Controls are essential; indeed, their importance is exacerbated.

The main conclusion is that despite technology having undergone many evolutionary steps, the fundamental principles associated with regulatory predicate rules and good engineering practices still, very much, apply and can be fully exploited.

In the current edition of the framework, the following topics have been further elaborated and outlined in documents on their own:

- Cloud Services – Pre Amble (this document)
- Cloud Services – Terminology
- Cloud Services – Audit Activities
- Cloud Services – Regulatory Requirements

2. Background and Acknowledgements

While cloud adoption has been robust in industries outside the life sciences and, to a growing extent, in some non-regulated areas of life sciences, many organizations adhering to good laboratory, clinical, manufacturing and distribution practices (GxP) are being challenged to scale-up their understanding, interest and adoption of cloud-based services.

There have been nine principal authors of these Cloud Framework Documents from across the industry – service providers, pharmaceutical companies and an independent consultant. In addition, some 30 other people have made various forms of contribution to the formulation of this document by way of review, case studies and general discussions. Special thanks should be given to:

- Gregory Purnsley, Biocryst
- Suzanne Studinger, QAS AG
- Daniel Dziadiw, Merck
- Robert Streit, Johnson & Johnson
- Evjatar (Evi) Cohen, Appian Corporation
- Anders Vidstrup, NNIT A/S

The first version of this Cloud Framework has been issued in 2013. Originally, the Pharmaceutical R&D Information Systems Management Executives Forum (PRISME forum) facilitated the creation of a working group to develop a framework on the topic of “lowering barriers to the adoption of cloud technologies in regulated life sciences organizations”. Ever since this working group has operated under the auspices of the Pharmaceutical User Software Exchange (PHUSE) and its collaboration with the FDA as part of the Computational Sciences Symposium.

Today, many intense discussions, meetings, and internal and external presentations later, this framework document has grown into a *guide* that has moved from addressing the blocking aspects limiting cloud adoption to pointing out the key elements for a successful adoption of cloud services in the regulated life sciences industries whilst complying with international regulatory standards.

3. Cloud Services – An Introduction

The use of cloud services is having far-reaching effects on organizations in academia, industry, and government, and the cloud services industry is evolving and changing rapidly in terms of technological innovation as well as how various stakeholders are deploying and leveraging cloud services for the benefit of their own organizations and business models.

Owing to the rapidly evolving cloud service industry, the term “cloud” is essentially jargon and is open to many different interpretations depending on knowledge, experience and perspective. Within the PHUSE working group, we have resisted the temptation to formulate new definitions, and instead, have built our thinking - and this framework - on real life examples and case studies, identifying success, failures, benefits, and pitfalls along the way.

Having acknowledged that a common starting point for understanding cloud is needed, we have leveraged the most frequently cited definition published in September 2011 by NIST ref [3], the National Institute of Standards and Technology, a federal agency within the United States Department of Commerce.

“Cloud computing is a model for enabling ubiquitous, 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”

This has been supplemented with definitions taken from ISO ref [2] in October 2014.

“Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.”

As such, the *cloud*, simply, refers to software and various IT services in one or across many data centers/facilities. Cloud computing is an evolution of online services and IT deployment models that leverages existing technologies like the Internet, service-oriented architecture, virtualization, relational and non-relational databases, deployment and test automation, identity and access management, and so on.

For further details on Cloud Terminology, see separate document from the Pharmaceutical User Software Exchange (PHUSE), Cloud Services – Terminology

3.1 Cloud Service Models vs. Traditional Computerized System

3.1.1 GxP Computerized System Context

The Life Science sector is regulated and governed by Good Laboratory, Clinical, Manufacturing and Distribution practices (GxP). In the context of GxPs, a *computerized system* [traditionally] refers to the “...combination of [computer] hardware, infrastructure software, software applications, and associated documents (e.g. user manuals and standard operation procedures) that create, modify, maintain, archive, retrieve, or transmit digital information related to the conduct of GxP operations” ref [5].

When computerized systems are used in support of laboratory, clinical, or manufacturing processes and handling of predicated data additional controls maybe required, and a risk-based approach is recommended.

In this context, the implementation of computerized systems, traditionally means/meant that the GxP organization purchases and installs the physical hardware, infrastructure software (operating system, database environment, application stack, etc.) and a GxP Application, or outsources some or all of these activities to a third party. When these computerized system components are installed inside the GxP-regulated organizations facility they’re said to be “on premises,” and when they’re installed in someone else’s facility and remotely accessed they’re said to be “co-located” or “externally hosted”.

Physical computer hardware and infrastructure software (“Infrastructure”) generally consists of commercial-off-the-shelf (COTS) products and services purchased “as is”. Since infrastructure is typically a general-purpose IT commodity sold in high volumes in the commercial marketplace, it is generally considered a lower risk component of the computerized system, despite security related issues often related to infrastructure elements. After installation, the GxP regulated organization configures and tests the infrastructure to verify and document proper operation; this is typically referred to as *infrastructure qualification*.

GxP applications installed on qualified infrastructure can be COTS or custom software and the level of controls usually depends on the intended use of the application and a risk-based approach. GxP applications are installed on the qualified infrastructure, configured for the specific GxP processes and procedures, and then tested to ensure the intended use and requirements are fulfilled; this is typically referred to as *software validation*.

This basic scenario of running applications installed on infrastructure was the predominant approach in GxP computerized systems until the popularization of hardware virtualization in the early to mid-1990s. Developed originally in the 1960s as a way to support time-sharing of mainframes, virtualization allows a single piece of computer hardware (i.e., server) to operate one or more virtual machines that operate independently and securely. This provides more efficient use of the physical hardware and greater flexibility to run different software programs and security groups in each virtual machine. The infrastructure component that makes virtualization possible is called a virtual machine manager (“hypervisor”).

3.1.2 Cloud Service Models

The following graphic depicts the basic elements of such an overall virtualized computer system in a “total stack” format geared toward GxP and its high-level aspects that are dealt with elsewhere in this document.

GxP Requirements	
GxP Organization	IT Policies & Standards
GxP Intended Use	GxP SOPs Process Validation
COTS/Custom Software	Software Operations Software Validation Software Purchasing/ Development Supplier Assessment
OS / Application Framework / Database Engines / Storage	Infrastructure Maintenance Infrastructure Qualification Infrastructure Purchasing
Virtual Hardware	
Hypervisor	
Physical Hardware / Networking	

Figure 1: Elements of a Virtualized GxP System

This trend toward virtualization combined with other technologies such as web services and deployment/test automation to deliver new capabilities and service models are nowadays recognized as cloud computing. With cloud-based infrastructure, this combination of technologies and cloud characteristics are used to abstract resources and controls between the self-service cloud resources (IaaS, PaaS, SaaS) and the underlying physical resources (hardware and facility).

What is the difference between a Virtual Private Cloud and a Public cloud, and who is accountable for the security in an externally hosted cloud environment?

A Virtual Private Cloud allows the configuration of a logically private cloud enabling “closed system” segregation for an organization in a Public Cloud provider’s environment.

Security in the cloud can be viewed similarly as Data Integrity controls. Consider:

- Security controls for external use should be no different than those applied for internally hosted systems.
- The customer owns the assessment of the cloud provider for appropriate security controls for the desired use cases, and ensuring customer’s security standards are met.
- Ongoing monitoring of environments deployed at a cloud provider to ensure policy enforcement, as well as supplier monitoring of their controls should be performed.

For more on contractual considerations, see [sections 4.1.1, 4.1.2 and 4.1.3](#)

Our IT department is looking to adopt external IaaS cloud partners as part of a new Data Center strategy. What steps to take to understand feasibility?

Establishment of a “Cloud Strategy” is critical to understanding requirements. Will you pursue Public Cloud? Is the company more comfortable with an in-house Private Cloud? Perhaps a hybrid solution for maximum flexibility? Regardless of the direction, the strategy must be championed by senior leadership with a clear desired end-state communicated.

No matter the model, a critical component to success is the deployment and adoption of Agile/DevOps tools and automation. This is a significant shift in IT infrastructure processes, and usually disruptive to legacy organization/ resources. Given the increased adoption by Life Sciences, this has become a requirement for cost effectiveness and efficiency. This should include adoption of Continuous Integration/Continuous Delivery (CI/CD). An organization assessment for necessary skills is highly recommended and likely result in sourcing skills/organizational changes. Skills requirements are not limited to IT but will also require the appropriate IT Security and IT/QA Compliance resources.

3.1.2.1 Infrastructure as a Service (IaaS)

IaaS refers to infrastructure resources being provided as a cloud service model. This includes virtualized servers and network devices with scalable processing capacity and reserved bandwidth for storage and Internet access, ref [1]. When IaaS is incorporated into GxP computerized systems, Cloud Service Customers retain a number of GxP responsibilities ensuring the qualification status of this infrastructure.

3.1.2.2 Platform as a Service (PaaS)

PaaS is similar to IaaS but also includes the required services for a particular application to work. In other words, PaaS is IaaS with runtime management and software components required for a given application to work on the IaaS. In PaaS, Cloud Service Brokers and Cloud Service Providers manage the IaaS responsibilities and the virtual infrastructure, and Cloud Service Customers manage the platform and application responsibilities.

3.1.2.3 Software as a Service (SaaS)

SaaS includes complete software applications provided as a cloud service. SaaS systems are typically accessed via a web browser and/or installed client applications. The application(s) run (and associated data is stored/processed) on PaaS/IaaS, responsibility for which shall likely rest with the SaaS Cloud Service Provider's organization (but, which, may be contracted by the SaaS Cloud Service Provider to one or more PaaS and/or IaaS Cloud Service Brokers and/or Cloud Service Providers). SaaS Cloud Service Providers sometimes provide – in whole or in part – their own PaaS/IaaS.

3.2 IT Supply Chain in the Cloud Era

Traditionally, customers within the life sciences sector have been accustomed to “owning” and having overall control of all aspects of a technology stack associated with the computerized systems that they utilize. In cloud-based solutions this concept is disrupted in that contracted Cloud Service Providers have responsibility for provisioning of different services within such a technology stack. And, therefore, the responsibilities are delegated from the customer to the provider(s) recognizing that the services from such providers may not be unique to the life sciences industry.

The supply chain of IT resources has grown over time from a simple, direct relationship between a purchaser and supplier to a set of relationships between purchasers, product suppliers, and service providers, as well as their downstream suppliers. The growth of Internet-based services and loosely coupled web services has further increased the complexity of computerized systems provisioning. The ability to manage this IT supply chain is now a critical success factor in business operations and compliance.

3.2.1 Cloud Roles

The terms used in cloud system roles are rapidly evolving as the cloud marketplace evolves, and for the purposes of this document we have identified the basic roles based, here, from NIST ref [3] and ISO ref [2].

- **Consumer / Customer:** In the context of GxP, cloud consumers are generally the organizations that purchase and use the cloud services to support their GxP-regulated activities. For example, a pharma company that selects and implements a

cloud-based LIMS as a SaaS solution for their GMP laboratory would be considered a cloud consumer. Cloud consumers are generally billed for the cloud services they consume, and depending on the services requested (IaaS, PaaS, SaaS) their activities, use cases and GxP requirements may vary.

- **Provider:** Cloud providers are the organizations or entities responsible for making the cloud service available to consumers. The activities that the cloud providers perform will vary depending on their particular service offerings and can include building, deploying, operating and maintaining the cloud infrastructure and associated service layers.
- **Broker / Manager:** Cloud managers are the organizations and entities that manage the configuration, delivery and use of cloud services on behalf of the cloud consumer. In the GxP context, for example, cloud managers may perform infrastructure change control activities on the consumers' virtual infrastructure built using general purpose, commercial cloud services.
- **Auditor:** A cloud auditor is a party that is qualified to conduct assessments of the cloud provider and the cloud infrastructure underlying the IaaS, PaaS, SaaS services. The auditor may be an independent third party such as a third-party assessment organization (3PAO) or can also be a member of the consumer, provider or manager organization.

3.2.2 Activities and Examples in the Cloud Supply Chain

In this framework, we have chosen to use the following roles/parties:

- Cloud Service Customer,
- Cloud Service Brokers, and
- Cloud Service Providers.

An organizational entity can play more than one role at any given contractual situation. The figure below provides a simplistic model. In the real world the cloud service providers for a solution often involve three or more SaaS and an IaaS provider.

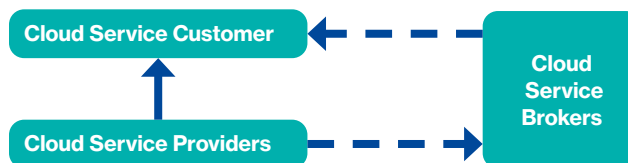


Figure 2: Connection between roles/parties in usage/provision of cloud services

3.2.2.1 Examples of Scenarios

It is important to understand the interactions between the roles identified in Figure 2. While there are many potential variations, three foundational scenarios seem to be the most common and can be used to illustrate how these roles and their responsibilities can interact.

Scenario 1

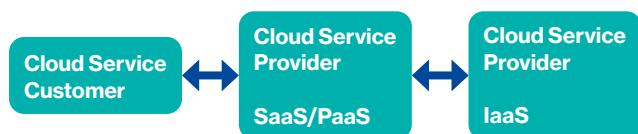


Figure 3: Scenario 1 example

- **Cloud Service Customer:** a pharmaceutical company who is the service consumer, with a contractual relationship with the Cloud Service Provider (SaaS/PaaS) only.
- **Cloud Service Provider (SaaS/PaaS):** a service provider who is providing the service to the Cloud Service Customer. This provider would have a direct contractual relationship with the customer and with the Cloud Service Provider (IaaS).
- **Cloud Service Provider (IaaS):** Providing the infrastructure services with a contractual relationship with the Cloud Service Provider (SaaS/PaaS) only.

In Scenario 1 the operational and contractual interactions follow the same path. In this scenario both Cloud Service Providers *could* be the same organization.

Scenario 2

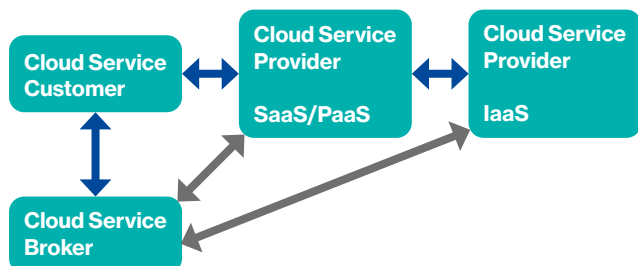


Figure 4: Scenario 2 example

- **Cloud Service Customer:** a pharmaceutical company, who has a contractual relationship (shown by the black arrows) with the Cloud Service Provider (SaaS/PaaS) and the Cloud Service Broker.
- **Cloud Service Provider (SaaS/PaaS):** a service provider who is providing the service to the Cloud Service Customer (shown by the black arrows). This provider would have a direct contractual relationship with the customer and with the Cloud Service Provider (IaaS) and, additionally, is subject to the operational controls of the Cloud Service Broker (shown by the gray arrows).
- **Cloud Service Provider (IaaS):** Providing the infrastructure services with a contractual relationship with the Cloud Service Provider (SaaS/PaaS) only and is subject to the operational controls of the Cloud Service Broker (shown by the gray arrows).
- **Cloud Service Broker:** An intermediary entity that has been delegated the operational responsibilities over the Cloud Service Providers by the Cloud Service Customer.

In Scenario 2 the operational and contractual interactions follow different paths with operational interactions (shown by the gray arrows) between the Broker, Provider (PaaS/SaaS) and Provider (IaaS). Again, both Cloud Service Providers *could* be the same organization.

Scenario 3

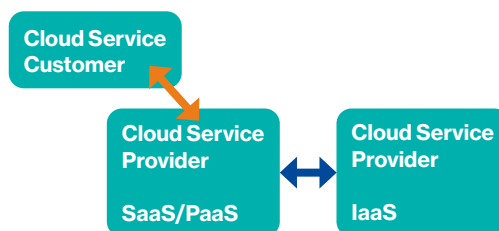


Figure 5: Scenario 3 example

- **Cloud Service Customer:** a pharmaceutical company who is consuming a service provided by the company's own IT organization (that is operating as a SaaS/PaaS provider).
- **Cloud Service Provider (SaaS/PaaS):** a pharmaceutical company internal IT organization who is using a Cloud Service Provider (IaaS) to provide an externally hosted private cloud. This pharmaceutical company IT organization would have a direct contractual relationship with the Cloud Service Provider (IaaS) and, typically, an SLA with their internal business customers (shown as the yellow arrow).
- **Cloud Service Provider (IaaS):** Providing the base infrastructure services with a contractual relationship with the Cloud Service Provider (SaaS/PaaS).

In Scenario 3 the contractual relationship is between the pharmaceutical company and the Cloud Service Provider (IaaS). All operational interactions are the responsibility of the internal IT organization of the pharmaceutical company.

3.2.2.2 Examples by Role

Below are examples of the activities that may be performed by each key role. This detailed table needs to be interpreted carefully because more-than one organizational party may undertake the roles of the left-most column. Conversely, a single organizational entity may also fulfill roles and responsibilities spanning the Cloud Service Customer/Cloud Service Broker/Cloud Service Provider "layers".

Qualification: Most cloud providers do not use the term qualification. Yet, in practice they are following the processes included in the GxP term "qualification".

General Audit Activities in the Cloud Supply Chain should be conducted. For further details, see separate document from the Pharmaceutical User Software Exchange (PHUSE), Cloud Services – Audit Activities

	IaaS	PaaS	SaaS
Cloud Service Customer	<p>Manages privileged and/or service accounts</p> <p>Defines and manages workflows supporting application needs</p> <p>Conducts additional qualification of infrastructure according to intended use</p>	<p>Manages privileged and/or service accounts</p> <p>Defines and manages workflow supporting application needs</p> <p>Conducts additional qualification of infrastructure- and platform according to intended use</p>	<p>Manages user accounts and roles</p> <p>Defines and manages workflow supporting application needs</p> <p>Conducts validation of applications according to intended use, include leverage of documentation to be reused/looked into as a part cloud user test/assessment/audit</p>
Cloud Service Broker	<p>Defines service requirements based on the approved service business case and the service risk assessment</p> <p>Assesses service risk</p> <p>Selects Cloud Service Provider on behalf of or together with the Cloud Service Customer</p>	<p>Describes service, including service level options</p> <p>Describes the architecture</p> <p>Defines cloud service provider KPIs</p> <p>Identifies relevant CIs based on the service risk assessment</p> <p>Evaluates the need for standards for the service on behalf of or together with the Cloud Service Customer</p>	<p>Releases service</p> <p>Ensures implementation of services by the Cloud Service Providers according to the defined service requirements and agreed service levels</p>
Cloud Service Providers	<p>Provides Customer Support.</p> <p>Provides handling of security and risk identifications and controls.</p> <p>Monitoring e.g.,</p> <ul style="list-style-type: none"> • security breaches, • backup jobs, • monitoring /auditing activities in the boxes for the Cloud Service Customer. And in turn delete there "manages privileged and service accounts" - the customer is not managing these accounts... 		
	<p>Provisions and manages the physical resources, builds and maintains the resource abstraction and control layer</p> <p>Qualifies Infrastructure services</p>	<p>Implements and/or deploys services according to the defined service requirements and agreed service levels</p> <p>Operates services</p>	
		Qualifies Infrastructure- and Platform services	Validates generic functionality in application

4. GxP Considerations for Cloud Service Customers and Cloud Service Brokers

When adopting cloud services for GxP uses, Cloud Service Customers and Cloud Service Brokers must review and evaluate the major control areas within their organization(s) that are impacted by the cloud technologies. These control areas will be covered below in relation to the organizational policies and procedures that are key to cloud adoption and implementation. One of the largest challenges in the GxP space for cloud adoption by Cloud Service Customers is to have the assurance that the Cloud Service Providers and Cloud Service Brokers are fully assessed in these key control areas.

When evaluating potential Cloud vendors, what should I look for in the vendor assessment to protect the company's data?

Review Cloud offerings and assess the impact to your company's model: public cloud, virtual private cloud, and/or private cloud

Review the vendor's qualification process for third party vendors to determine the cloud responsibilities and liability

For more on contractual considerations, see [section 4.1.1](#)

Before adopting the cloud, my company wants to understand where our data will be stored, and if we can control the physical location of data?

As the potential customer, you need to first understand the regulatory/privacy classification of the data in scope. This then defines the requirements to ask the right questions of potential Cloud vendors of which data center locations can be part of the solution, and how that vendor implements controls for data storage/access.

If concerned about the location of "original electronic data", it's still an architecture discussion. Based on your design, where are the original records generated and stored? If the design, proposes cloud, then you need to assess the vendor.

For more on contractual considerations, see [section 4.1.1](#) and [4.1.2](#)

My company has an application need (GxP process/solution), and would like to adopt a vendor provided SaaS platform. The vendor claims to have some customers that are Life Science companies. How do I proceed?

Once you've begun to document your software user requirements, engage your IT Quality and/or Supplier Management resources. An audit/assessment of the vendor's solution should be the first step. Life Science customers may be using the solution, but not for GxP purposes, so it is important to determine the extent any GxP usage.

Verify the concept of the desired SaaS solution from the supplier perspective. Is it based on a Service Broker model, or a Service Provider-Broker model?

For more information, see [section 3.2.2](#)

You should determine where the solution is hosted prior to the audit or assessment. Is it the vendor's data center? Is it a sub-contracted 3rd party data center? Where is the data center(s) located?

- If the vendor is the host, you will need to assess the data center controls for security, building management, etc. in addition to the supplier's software Quality Management System and Software Development processes
- If a 3rd party, you will also need to diligently assess the SaaS vendor's Supplier Mgmt. process/controls. Did they perform a robust review of the data center controls? Do they have contractual compliance requirements in place with the sub-contractor?
- Location of the data center is important depending on a) application use case and b) potential Privacy concerns
- External assessment reports from qualified 3rd party resources may be adopted as input, i.e., SOC or ISO reports in relation to security and quality controls.

For more on audit/assessment considerations, see Cloud Services – Audit Activities document

Should the results of the audit/assessment be satisfactory, proceed to the establishment of the contract with the vendor. Care should be taken to ensure based on your use case that critical compliance requirements of the vendor are included. It may also be possible to include identified opportunities from the audit/assessment considered to be non-critical as deliverables.

Ensure that the ongoing ability to audit/assess vendor's processes on an agreed upon frequency as well as "for cause" situations are included.

4.1 SDLC Policy - Cloud Specific Guidance

Overall success in implementation of a cloud service is often dictated by the successful adoption and application of a customer's system-lifecycle (SDLC) policies and procedures to the cloud service/system.

System Implementation/Validation – The Cloud Service Customer's SDLC policy is the primary policy that defines, and sets forth, the requirements and procedures to implement and maintain a computerized system. This policy also ensures compliance with applicable laws, regulations, and company policies such as GxP.

Although it is beyond of the scope of this document to define an SDLC policy, the SDLC policy at a Cloud Service Customer defines an overall framework often made up of phases from project initiation and planning, through requirements, design, build, test, install, operation and retirement.

As defined in the FDA Glossary of terms: System Life Cycle – *'The course of developmental changes through which a system passes from its conception to the termination of its use; e.g. the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system.'* ref [4]

Some of the most crucial aspects of the assessment process are defined in the early stages of the consumer's overall SDLC policy framework, often referred to as the 'Planning Phase' or equivalent. During this key SDLC phase, the following items are initiated including;

- Supplier Management and Assessment
- Information Risk, Privacy and Data Assessment
- IT Security Evaluation.

Due to the importance of these topics, they are explored in greater detail in the following three sections of this chapter.

Another challenge in the planning phase of a GxP cloud-based solution is that, many times a good portion of the information, or other SDLC artifacts, may reside with the providers or managers, yet the overall accountability for the GxP system lies with the Cloud Service Customer. Therefore, Cloud Service Customers will need to work closely with the Cloud Service Providers/Cloud Service Brokers to establish a process in which this information can be referenced, leveraged and/or managed from within their SDLC policy.

In addition, provisions will need to be made to ensure that these SDLC artifacts can be provided upon request from the Cloud Service Providers/Cloud Service Brokers, during, for example, a regulatory inspection of the Cloud Service Customer. This may be true of project artifacts in the overall implementation of the system, or key operational system control process in the following areas:

- | | |
|----------------------------|---|
| • Configuration Management | • Identity and Access Management |
| • Change Management | • Back-up and Restore |
| • Problem Management | • Business Continuity and Disaster Recovery |
| • Incident Management | |

It is essential that the Cloud Service Customer's SDLC Policy accurately and meaningfully reflect the roles and responsibilities of the various Cloud Service Broker and Cloud Service Providers that are applicable.

Cloud-based implementations should be viewed like any other system implementation. The overall SDLC is the key policy to the success of implementation and operation of a cloud-based solution. However, application of the SDLC to the specific nature of cloud is also a key to success. The tailoring of the SDLC approach to cloud is highly dependent on the topics that follow, and their application to cloud. It is often in the early stages of the SDLC (i.e. Planning phases) in which these activities are initiated and addressed by the Cloud Service Customer with the Cloud Service Providers.

SDLC Cloud Guidance and Governance - It is the intent of this document to provide high level, and non-prescriptive guidance, to help in the adoption of cloud. We recommend that Cloud Service Customers develop their own specific policies and approach to cloud adoption. Specifically, how to apply the customer's SDLC policy to cloud in order to ensure a holistic GxP-compliant solution is one of the factors that will assist in appropriately and consistently applying this methodology for regulatory purposes. Such guidance will help in the transition to cloud while maintaining a manageable, secure, regulatory compliant and policy compliant environment.

The guidance may serve as a reference for critical decision-making across topics such as network topography, security capabilities, and leveraging the information risk and guide compliance teams to safely enable business initiatives in the cloud.

Cloud Service Customers and Cloud Service Brokers, particularly those at organizations operating in multiple locations, should discuss the extent and manner in which they want to leverage cloud services both in their business in general as well as in the context of GxP activities. An overall Cloud Governance body can oversee this strategy and monitor key factors like cost, risk and regulatory exposure.

Infrastructure/Platform Qualification: In GxP environments, Cloud Service Customers must be able to demonstrate that the infrastructure and underlying platforms are qualified. 'Qualification' is a legacy term, but in practice is a set of stages in the documented SDLC process covering testing, validation of an install, and documentation of completion of these processes. When applied to a platform, or infrastructure, this process ensures the underlying components that support regulated applications are appropriate for their intended use.

As part of the SDLC, the Qualification strategy for a platform or infrastructure is often a set of deliverables required for regulated business applications. It frequently includes:

- Quality Assurance or Qualification Plans, Requirements and Design/Configuration Specifications (e.g., Technical Standards, Degree of customization required, parameter settings)
- Installation qualification and operational qualification (IQ/OQ) for infrastructure. The industry sometimes uses other terms to indicate these testing processes such as 'verification' to

reduce confusion with process validation activities.

- Formal Agreements (e.g., Service Level Agreements (SLAs)/ Operating Level Agreements (OLAs))
- SOPS governing specific Infrastructure or Platform processes.
- SOPs governing Infrastructure's approach to the support of GxP applications
- Documentation of the infrastructure, including manuals, usage instructions, and processes for knowledge management
- Disaster Recovery and/or Business Continuity Plans for critical services/infrastructure utilities.

When applying these qualification processes to a cloud infrastructure, it is important to understand the layers of the cloud, and ensure the proper controls are qualified at each layer. For example, an application could be installed on a reusable machine image from which instances are launched. The machine image must be qualified for use in a GxP environment. The qualification activities for the image are distinct from any activities that must be performed for the instances that are created from it. There may be scenarios, where it isn't possible to adopt documentation from a Cloud Service provider on specific part of the service. In that case a proper risk assessment must be conducted.

As noted previously, some of this information may reside with the Cloud Service Broker. Therefore, Cloud Service Customers will need to work closely with their Cloud Service Providers or Cloud Service Brokers to create a process in which this information can be referenced and managed or provided upon request during a regulatory inspection.

4.1.1 Supplier Management Policies

Cloud service models typically involve external "IT service suppliers" of various forms that provide both services and systems. In addition, reliance on the Cloud Service Provider or Cloud Service Broker will be critical during the operational phase of the system and service.

Therefore, key policies around management of these types of cloud suppliers become paramount.

Supplier IT Practices Assessment - The competence and reliability of Cloud Service Brokers and Cloud Service Providers are key factors when selecting a cloud system/service. As such, each should be formally and rigorously assessed and documented by the Cloud Service Customer on an ongoing basis. The documentary artifacts should be available upon request, as this is an expectation of regulatory agencies for all systems supporting regulated business functions. A separate Cloud Service Auditor may be engaged to perform this activity.

As Cloud Service Brokers and Cloud Service Providers provide both services and systems, the overall assessment process will require an analysis of both. As such, an assessment must focus on both the internal practices of the providers to develop and maintain the systems, as well as relevant supplier practices, including their quality system, etc., needed to support the services. This general assessment practices would be initially

assessed, and then re-performed on an agreed to periodic basis typically covering areas such as the following:

- Personnel and Background Verification
- Training
- Software Development Life Cycle Methodology/ Project Management
- Quality Assurance/Control Practices
- Change and Configuration Management
- Error Detection/Problem Resolution (Incident/ Problem Management)
- Backup/Restore
- Performance Monitoring.

Effectiveness of Controls and Auditing - Regulatory authorities, partners, and clients may perform audits of GxP systems to ensure compliance. By the nature of cloud computing technology, physical audits of computing resources managed by a cloud service loses its value as there are no dedicated physical computing resources.

The fact that physical resources cannot be visually inspected does not mean there is nothing to inspect. Periodic or continuous review of control objectives may replace this activity and provide significant benefit. In accordance with supplier contracts and agreements, a periodic review may include external or third-party assessments of the provider in addition to the assessments conducted by the customer (i.e., IT Practices, Information Risk, and Privacy).

A cloud customer or broker may periodically review materials provided by the cloud provider such as:

- Performance Monitoring Indicators and related support cases and incidents
- 3rd Party Independent Audits
- Industry Certifications
- Quality Manual

In addition, continuous or semi-continuous review of control objectives may include monitoring and alerting of the cloud environment, including such measures as application performance, unusual patterns of data access, or daily verification of accounts against configured policies.

Procurement/Contracts – Procurement departments take on an important role in establishing a commercial relationship between companies, negotiating costs, and formalizing legally binding contracts. A key item will be establishing the formal contract between the Cloud Service Brokers and Cloud Service Providers and Cloud Service Customer known as the underpinning contract and described in the next section. It should be noted that most of this activity is normally outside of the SDLC policy; for example, excluded from SDLC would be assessment and management of commercial terms such as Insurance, Intellectual Property, Dispute Resolution, Payment terms, etc.

Supplier Agreements - Clear understanding of service commitments and responsibilities are required throughout all cloud systems and services to ensure proper support and use of business processes, and the expectations of regulatory agencies. This is important in the adoption of cloud due to the complex nature and interdependence of Cloud Service Customers, Cloud Service Brokers and Cloud Service Providers. This understanding is required for effective functioning and

compliance of business operations via the cloud systems and services. In addition, as mentioned, third parties operate much of the overall cloud solution.

Agreements to define this understanding are essential to support these interactions. The requirements around the agreements need to consider the customer's desired outcomes, including functionality and service/operational level targets. These agreements and requirements may fall into the following categories:

- Service Level Requirements – The clients' desired outcomes, including functionality and service level targets. These service targets define the individual level of service to achieve which may include terms and conditions, goals, costs and milestones. They also define the impact cost of missed targets and can be related to Service Level Agreements (SLA's), Operational Level Agreements (OLA's) or Contracts.
- Service Level Agreements (SLA) – Agreements between the customer and manager/provider defining key service targets and responsibilities.
- Operational Level Agreement (OLA) – Agreements between internal customer and/or manager functions and the provider that defines the working relationship and expectations in support of the SLA.
- Underpinning Contracts (UC) – A formal contract between the Cloud Service Customer/Cloud Service Broker(s) and the Cloud Service Provider(s) that defines key service targets and responsibilities required to meet the SLA. Terms of the SLA or OLA should remain consistent with any UC's. In some cases, the SLA and OLA may be part of the UC; however, how to best structure these agreements will also depend on how the system and service is managed based on the arrangement of the Cloud Service Customer, Cloud Service Brokers and Cloud Service Providers.

In general, each agreement would include compliance and service targets, milestones and actions. It should be noted that agreement terms specifically around GxP requirements may be incorporated into the categories listed above, or an agreement focused specifically on GxP requirements (i.e., "Quality Agreement"). A target would include what is measured, including criteria.

4.1.1.1 Quality Agreement Considerations

When Cloud Service Customers, Cloud Service Brokers and Cloud Service Providers form Agreements they need to consider numerous factors in terms of GxP compliance in and around the core aspects of:

- Services scope
- Defined operational activities.
- Roles, Accountabilities and Responsibilities.

To formulate such agreements, the following checklists of topics should be considered were possible.

Service Description

- Service Scope – Defines the scope of services covered by the agreement, primary users and other users. Service scope may include the following;
 - Change Management
 - Configuration Management
 - Incident and Problem Management
 - Service requests (i.e. ad-hoc)
 - System Administration
 - Security and Account Management
 - Performance Monitoring – including Corrective and Preventative Actions
 - Maintenance
 - Periodic Review - Service level monitoring and review
 - Training
 - Testing
 - Backup/Restore and Archival/Retrieval
 - Vendor & Process Quality
 - Application Development
 - Customization Development
- Solution Scope – Defines the scope of the IT solution including all IT assets including items such as GxP relevance, Primary Locations, etc.

Roles, Responsibilities, and Contacts

- Customer Responsibilities
- System Support Responsibilities

Service Definitions and Procedures

- Support Services and Scope – Defines the support tiers, covered services (i.e. change management, security access), assets in scope, and procedures.
- Service Level Classifications - Defines the standards and target metrics for the services.
- Service/Application Availability - Defined as the time when a service is expected to be available for customer use (normally not guaranteed outside the defined Support Hours)
- Support/Coverage Hours - Defined as the time period when support personnel are expected to be available to address incidents or service requests.
- Incidents / Service Disruption - An incident is defined as any event which is not part of the standard operation of a service, and which causes, or may cause an interruption to, or a reduction in, the quality to that service depending on the level of severity. The Service Level determines response and resolution times for each severity level.
- Response Time - Defined as the time it takes for the support team to acknowledge to the client that they have received the incident.
- Resolution Time - defined as the time it takes to restore a service back to the agreed upon Service level.
- Service Requests (Non-Discretionary) – Resolution time to address unscheduled requests which may arise (i.e. request's arising from a Health Authority).
- Problem Management – Time to disposition a problem, typically arising from one or more related system incidents.

Maintenance and Service Changes

- Defining how changes to Agreement(s) must be authorized. Example of changes includes change in scope, changes in services offered, or changes to performance metrics.

Monitoring, Reporting and Reviewing

Many large cloud providers expect the customer to monitor their specific VMs/instances, as the provider focuses on the overall cloud/primary service availability. The following must be taken into consideration:

- Standard Monitoring and Reporting – Defines monitoring and reporting requirements around information such as daily site system availability, unplanned downtime, etc.
- Ad Hoc Reporting (Service Request) – Defines monitoring and reporting of these service requests.
- Service Review Meetings – Defines necessary reviews of agreement(s) (i.e. Review Board, Audience, and Frequency).

4.1.2 Information Risk Management, Privacy and Data Protection Policies

Risk management is a key activity in the overall analysis of risks for a GxP cloud implementation. This is typically a key input of the SDLC, initiated in the Planning phase and fully vetted before progressing the solutions to the production/operational environment.

Risk Assessment - Risk Assessment is the overall assessment and identification of the Cloud Service Providers' risks. Output of such assessment may include high-risk findings that need to be mitigated and/or remediated prior to implementation. The scope of this assessment often includes risks to:

- Information
- Hardware
- Software
- Policies and processes

that handle or store information. The risk assessment process also takes into account the risks to the:

- Confidentiality
- Integrity
- Availability

of information and systems as well as compliance with laws and regulations. Through a systematic, disciplined risk assessment process, GxP Cloud Service Customers can ensure that information security requirements are considered to ensure compliance with all appropriate security requirements (often driven by law), protect information throughout its life cycle, and facilitate the efficient implementation of security controls.

The output of this process is often input to the consideration of overall security provisions of the Cloud Service Provider.

Privacy Assessment – Although not an explicit GxP requirement, considerations for Privacy, and how PII (Personally Identifiable Information) is handled by the cloud solution has become a key topic for assessment for all systems. A key consideration for cloud is where the actual PII is physically stored and, indeed, who has access to it. Such considerations impact proper compliance to Privacy Regulations, especially since cloud solutions are often not geographically static.

Data Protection Assessment - This involves the appropriate classification and handling of all of the Cloud Service Customer's data and information. Proper tagging, classification and

ownership of data greatly assists the Cloud Service Customer's security controls to enforce the right rules and that documents are properly classified but are also required to ensure proper data use consent. When cloud services are used in clinical research, for example, human subject protection regulations require that the safety and privacy risks to the human subjects are reasonable in relation to the anticipated benefits. For instance, clinical research Sponsors and Investigators must provide external parties (e.g., ECs/IRBs) with evidence to demonstrate the system is well controlled and that potential safety and privacy risks are appropriately managed.

The European Global Data Protection Regulation (GDPR) is in effect as of 25 May 2018. While it does not specifically focus on cloud installations (the word 'cloud' is not mentioned anywhere), it does contain several clauses that have a huge impact on the way companies collect, manage and store their data. It falls outside of the scope of this document to assess the impact of the GDPR specifically for cloud installations. By now, most companies will have performed a GDPR assessment, acting where needed by adjusting and sharpening their policies and/or the way their 3rd parties handle data management on behalf of the company. Cloud consumers that collect and process EU citizen data, even if they are not from the EU, have to adhere to the regulations of the GDPR, and this is something that must be taken into account when selecting a provider.

The GDPR sets forth many requirements that are not so easy to manage, specifically for a cloud installation. Most notoriously, chapter 3 entitles so call 'data subjects' a whole set of rights around strengthening data privacy, for example the 'Right to Restriction' (Article 16) and the 'Right to Erasure' (Article 18). Citizens can demand to see what data is held on them, to what purpose, and they may demand that data are deleted at any time. The cloud service must provide sufficient functionality and controls to enable cloud customers to respect the GDPR regulations.

Additionally, the GDPR has requirements with regards to data sovereignty. It requires that all data stored on EU citizens are either stored in the EU region, or somewhere else with at least equal or better levels of protection. This requires a cloud consumer to be aware at where their data are localized. Many cloud providers provide flexible data localization options (based on fee), so with some negotiation and contracting it is usually possible to ascertain that data are stored in a location that complies with GDPR regulations.

My company decided to change our platform to a new Cloud Vendor, what steps are the major considerations in planning the data migration activities?

Scenarios:

Legacy to Cloud - When forming your data migration plan, consider your Cloud adoption plan for new trials as well as make decisions on the legacy study data: Which studies continue to support new clinical trials and programs? How will the company maintain/retire the legacy data and platforms? Plans to reduce the maintenance investment on legacy systems and plans to decommission while ramping up the Cloud platform adoption.

Cloud to Cloud - When forming your data migration plan, consider your Cloud to Cloud adoption plan: How will this migration occur? Where are each vendor's responsibilities? How will the company maintain/retire the former Cloud data or migrate all data to the new Cloud platform?

4.1.3 Cyber Security

Facilitating a transition to cloud while maintaining a secure regulatory compliant and policy compliant environment is one of the largest areas of concern in the adoption of cloud for GxP. A guide to the overall security considerations is a key reference for critical decision-making across topics such as network topography, security capabilities, and leveraging security and compliance to safely enable GxP business operations in the cloud.

In general, many of these control requirements are typical and consistent with other types of non-cloud technology implementations.

Implementation of cloud security is best viewed through a "shared responsibility model" which can be applied very differently than in a traditional on-premises datacenter model. Security in general requires applying layers on top of layers to maximize protection (many of these layers are briefly described in this document). This is needed regardless of whether we are in the cloud or a more traditional architecture. However, cloud implementations require that at least several of these layers are done as part of a shared model by the cloud provider or broker, as opposed to the more traditional ownership models. Security delegated to the cloud provider/broker still requires oversight from the customer including:

- Customers should assess the quality of the controls that cloud providers use to meet their responsibilities.
- Customers should seek to understand the full set of controls that are providing security -- it's the design and operation of some controls that are the responsibility of the cloud provider.
- Cloud providers often publish reports that cover their expectation of controls on the customer side (user entity controls). Customers should ask for those and understand what the cloud provider sees as out-of-scope for their responsibility.

Some additional points regarding cloud security which may differentiate it from more classical arrangements:

- As noted, Cloud is shared responsibility model. Much is handled by the Cloud Provider/Broker that the Cloud Consumer is not

responsible for. This responsibility of the customer reduces even more as we move from IaaS to PaaS and SaaS. However, a careful security design is required for cloud as equally as on premise.

- Cloud offers a number of readily available out-of-the-box security tools that can be quickly turned-on and implemented.
- Cloud is API based by nature. This makes automating and auditing much easier.
- Public cloud has shared tenancy requiring additional controls irrespective of fencing the environment and/or connecting back to the company network.

As such, the adoption of cloud for GxP operations has to consider implementation-specific security requirements in order to bring the business value to the Cloud Service Customer, and the broader security considerations to protect the assets and intellectual property of the Cloud Service Customer.

Implementation specific Security Requirements – These considerations are typically aligned to the requirement artifacts created as part of the SDLC process. This may include both technical controls required for the implementation (i.e., authentication methods such as 2F), but also user-based or other types of functional security requirements. This may include such items as security profiles to properly implement segregation of duties, requirements around maintaining data integrity, or privileged user access profiles.

Cloud Security Requirements – Overall security infrastructure considerations take a broader look at the overall security picture and their core elements in order to properly protect information and assets. Cloud Service Customers will need to evaluate their enterprise information security infrastructure at many of their core elements to ensure that their adoption of a Cloud Service Provider is fully vetted. The evaluation typically includes the assessment of available external certifications (HIPPA, Socs, ISO).

Internet - Internet connection points facilitate several important and necessary business processes and establish presence on the Internet from the perspective of users in the Cloud Service Customer, the Cloud Service Broker and the Cloud Service Provider. Elements of security protection in this regard include:

- Distributed Denial of Service (DDoS) Protection (protection from bandwidth consumption attacks)
- Web Application Firewall to protect publicly facing websites from various methods of attack (hacking, defacement, etc.)
- Guest Wireless Access to the public Internet
- Secure remote access to the network for employees
- General access to public and partner facing websites.
- Third Party Services (connections to third parties)
- Website Vulnerability Scanning.

Perimeter - The perimeter region is typically defined as the secure area that resides between the public Internet and the internal consumer network. It is commonly referred to as a DMZ and is there to help protect the consumer's network from external attacks, while providing key externally facing services for the business. Elements of security protection in the perimeter region include (but not limited to):

- Firewalls – allowing only permitted traffic into and out of the internal network

- Intrusion Detection Services - detection and prevention of attack traffic
- Secure Web Gateways and Proxies to provide a safe browsing experience for employees and external partners such as Health Care Providers.
- Network Data Leakage Prevention (DLP) Services – detection and prevention of the
- Unintentional leakage of sensitive data
- Secure Email Services

Internal Network - The internal network is primarily used to facilitate data and voice communications for various applications around the world. It connects corporate offices, manufacturing plants, research sites and most of the other business areas of the company. Elements of security protection within the internal network include:

- Firewalls
- Network Behavioral Analysis
- Vulnerability Scanning of most infrastructure components and applications.
- Intrusion Detection Services for key manufacturing locations and application environments
- Devices that connect to the network, such as employee laptops, desktops and servers require a good level of security protection. Elements of this endpoint security protection are:
 - Antivirus services to detect and remove malicious files.
 - Data Leakage Prevention to detect and prevent unintentional leakage of sensitive data.
 - A Host Firewall used to control and restrict access to only permitted areas within the network.
 - Policy Assessment
 - Encryption services used primarily used to protect data in the event of loss or theft of a device, and to ensure regulatory compliance where mandated.
 - Logging and Monitoring capabilities.

Management & Control Layer - This management and control layer contains all of the various configuration and reporting services that are required for ongoing operations and sustainment of security controls at all layers. These services are strictly controlled and only allow connections from those administrators who are permitted to manage and monitor security controls.

Data Management - Proper tagging and classification of data greatly assists the Cloud Service Customer's security controls to enforce the right rules based on the detection of this information on an endpoint machine or the network.

Service Management - Service Management pertains to the ongoing operations and continuous service improvement for all of the security controls in the different layers. It includes tasks such as user trouble call resolution, periodic system health checks, routine system upgrades and improvements, appropriate performance monitoring and reporting and regular discussions with the Cloud Service Providers and ongoing sustaining support of the infrastructure that provides essential security services.

4.2 Continuous Delivery and Continuous Validation

In this position paper we are intending to provide guidance, share best practices, and create a dialogue for professionals working and practicing in the Life Sciences domain specifically leveraging cloud-based Platform as a Service (PaaS) and

Software as a Service (SaaS) business solutions in the delivery and quality assurance of computerized systems that impact the storage and management of predicate records governed by predicate rules.

Of specific interest is the discussion of what it takes to establish trust and manage risk in three specific objectives of IT service management:

- Data Integrity
- Availability
- Usability, include validate secure state.

Achieving the management of risk to the above three IT service management objectives is also highly dependent on Infrastructure as a Service (IaaS) capabilities and was covered by previous position papers.

Computer Systems Validation practices are well established in Life Sciences, and the industry is expected to adhere to critical computer system validation standards and practices. Companies are required to meet strict standards, explicit and implied, in current good practices (GxP). These include planning, verification, testing, traceability, configuration management, integrating software life cycle management, and risk management activities.

4.2.1 The Challenge

Life Science companies – sponsors of medicinal products and medical devices, and combinations thereof – carry the ultimate responsibility for the efficacy and quality of their products. This is clearly delineated in current regulations. It also makes sense from a trust perspective as well as aspects of corporate responsibility and reputability.

The combination of dramatically faster pace along with an ever-increasing interdependence across business functions creates a critical need for integration and interoperability. This higher level of complexity creates risk and more opportunities for errors and miscommunications. Downstream, that impact can be dangerous: lapses in quality can impact the safety and efficacy of our medicines and medical devices. It is incumbent on the industry to exercise exceptional diligence over the core processes and systems that help get work done to prevent these errors from happening.

Our increased dependency on information systems is also challenging the boundaries of current interoperability and system integration, as well as the capabilities of existing COTS and in-house IT professionals to continue delivering on the promise of such information systems while delivering to very high standards and managing the risk in the following three key areas:

- Data Integrity
- Availability
- Usability, include validate secure state.

Life Sciences companies have been turning to cloud-based platforms to alleviate some of the pressures. This trend seems to continue accelerating. This is where trust and risk management become critical. ***Life Science companies must be able to establish trust in cloud-based systems and gain a solid understanding of the way cloud system providers are diligent***

in managing risk across the three key areas of Data Integrity, Availability, and Usability.

Could base platforms make it possible to provide for **continuous delivery** of software updates that either deliver new functionality and features, enhance existing features, or work to fix and alleviate software bugs as they are discovered or reported.

4.2.2 The Approach

The overall approach to establishing trust and trustworthiness in the continuous delivery of quality business solutions provided as PaaS and SaaS should be based on the basic notion of trust but verify.

First, the responsibility for software quality assurance in a continuous delivery model depends on the establishment and adherence of best practices by the PaaS or SaaS vendor (more on this below).

Second, since the overall responsibility for the medicinal product quality relies on the sponsor, the sponsor is still required to adhere to the applicable vendor audit regulatory requirements. In this case, such audits would cover the evaluation of evidence supporting a rigorous Software Development Life Cycle (SDLC) coupled by established Software Quality Assurance (SQA) and Software Quality Control (SQC) processes as part of the continuous delivery model.

The notion of trustworthiness of a vendor providing PaaS or SaaS via a continuous delivery model would emerge from positively passing supplier assessments. Initially, this would be likely conducted by individual clients, however, we could envision this evolving and migrating over time, towards a model whereby vendors would be evaluated for their continuous delivery model and execution, by a centralized acknowledged body. This model would follow the same principles followed by security SIGs (Standard Information Gathering) questionnaires.

The approach, of establishing trust and trustworthiness, in companies and vendors providing PaaS and SaaS business solutions, based on periodic review of their overall culture of quality and organizational excellence (CQOE). Aspect of the overall approach – organizational level analysis coupled with a product level analysis – should be applied to evaluate the fitness of a continuous development approach, which could bridge the gap between a Computer Software Validation approach, which is tied to what is known as the “Waterfall” approach and Computer Software Assurance approach, which benefits from an Agile software development approach leveraging Scrum methods.

Of critical importance is the adherence to Software Development Life Cycle (SDLC) best practices coupled with a rigorous Software Quality Assurance process. In a continuous model, this would further encompass **multiple quality** gates in combination with the establishment of a software development process that benefits from an equivalent to an “Andon Cord.” In manufacturing, the term Andon refers to a system which notifies managerial, maintenance, and other workers of a quality or processing problem. The alert can be activated manually by a worker using a pullcord or button or may be activated automatically by the production equipment itself. In the case of software development, any member of the software product development team can raise a flag and stop the continuous

development process in case of a quality or development process issue.

The SDLC framework should be tightly integrated with the quality unit, and benefit from its adaptable approach to planning, implementing, releasing, testing, and supporting software that is subject to on-going internal and external evaluation procedures and processes that ensure and provide a high level of confidence that the GA software meets its objectives and intended use efficiently, effectively, and securely. The software should not be considered Generally Available (GA) until it has successfully passed a series of QA validation procedures including the categorization of defect severity and defect priority, on an ongoing basis – as well as a battery of tests including endurance tests, stress tests, security, platform compatibility tests, and regression tests, which in a continuous delivery model are run and executed on a regular cadence.

4.2.3 DevOps

A definition of DevOps comes from Microsoft – “A compound of development (Dev) and operations (Ops), DevOps is the union of people, process, and technology to continually provide value to customers”.

Effective adoption of the public cloud (specifically IaaS/PaaS) requires a competent DevOps team, experienced in both Cloud technologies and automated software deployment & testing. Providers are continually releasing new services. For proper and timely adoption of such new services and capabilities, the DevOps teams must partner with Information Security to establish proper roles and appropriate access controls. Also, the team should consider defining standard configuration settings and methods for how the specific service instance would be backed up and restored, plus considerations for long term data retention – some retention schedules may call for up to 25 years retention period in Life Sciences.

During acceptance testing of new functionality, addition capabilities, update, and hot fixes, automated software testing is vital to executing a truly agile DevOps process. It can greatly shorten the time to qualify a new service. Even more importantly, an automated regression suite provides for rapid 100% testing when updating features to the overall Cloud Management Service.

Additional details on standards for DevOps may be found here –

- [IEEE 2675-2021](#) - IEEE Standard for DevOps: Building Reliable and Secure Systems Including Application Build, Package, and Deployment
- [ISO/IEC/IEEE 32675:2022](#) - Information technology – DevOps – Building reliable and secure systems including application build, package, and deployment.

4.2.3.1 Configuration Management

The configuration management process for Cloud Solutions must ensure that systems are created and managed appropriately in accordance with best practice standards:

- **Identify configurable items** such as servers and respective operating systems and software applications installed.
- **Create the baseline build of configuration items** using principles of least privilege and segregation in components and configurations; only essential capabilities are enabled, and components are broken down by function; this may be ensured

through automation. Each new baseline that is created is versioned and maintained.

- **Ensure secure configurations are applied to configuration items** through a change control process and automation.
- **Maintain and verify the baselines and configurations;** work together with the Information Security Team to ensure that there are no significant deviations between the baseline configuration and the operational environments and establish monitoring is in place.
- **Perform continuous system monitoring** to verify the continued implementation of security controls within the system; ensure that only authorized AMLs are accessing the systems; the information security team should also scan the cloud instances for any installed software to ensure it does not deviate from the baseline.

The configuration management team should maintain awareness and monitor the following:

- Support tickets from customers
- New laws or regulations applicable to Cloud
- Patches or vulnerability fixes for software in use
- Changes based on identified risk factors.
- New features or enhancements to the system
- Incident monitoring

Changes to the systems should go through a Change Management process where changes are classified and sent to a pool of approvers; the approvers verify the validity of the changes and approve the maintenance window. When a maintenance window is approved and scheduled the authorized support contacts nominated by the customer are notified. When the time of the maintenance window comes, the maintenance automatically applies the change upon reboot. The customer/ sponsor should be notified before any maintenance and at the time the maintenance starts and completes, in accordance with predefined SLAs.

Maintenance windows requested by the customer should be coordinated through support cases; those that are initiated by the Cloud team are coordinated through a formal notification process and can be discussed via support cases if necessary.

New features and automations in the Cloud are subject to the SDLC which in collaboration with the Information Security Team must undergo a security impact analysis review for significant changes.

During the SDLC process for building automations that orchestrate the life cycle of Cloud sites, there should be segregation of responsibilities; Cloud Architects should be responsible for merging and deploying back-end code changes to PRODUCTION while the Cloud Operations team members should be responsible for performing deployments of frontend artifacts to PRODUCTION. These changes should be reviewed by the deployers after they have been peer reviewed by a Senior software Engineer.

4.2.3.2 Change Management

Managing change effectively is crucial when implementing DevOps practices. Some key considerations and best practices for change management in a DevOps environment are:

- **Establish a Change Management Process:** Create a structured process for managing and tracking changes. Define roles and responsibilities, establish clear guidelines, and document

the steps involved in requesting, reviewing, providing impact assessments, approving, and implementing changes.

- **Automated Deployment and Infrastructure as Code (IaC):** Leverage automation tools and practices to deploy software and infrastructure changes consistently and reliably. Infrastructure as Code (IaC) enables versioning, testing, and automation of infrastructure changes, ensuring reproducibility and minimizing manual errors.
- **Continuous Integration and Continuous Delivery (CI/CD):** Implement CI/CD pipelines to automate the build, testing, and deployment processes. This allows for frequent and small changes to be integrated and delivered rapidly, reducing the risk of large-scale disruptions.
- **Version Control:** Utilize a version control system to manage code and configuration changes. Version control allows teams to track changes, collaborate effectively, and roll back changes if necessary.
- **Monitoring and Feedback Loops:** Establish comprehensive monitoring and logging mechanisms to gain visibility into the performance and stability of the system. Implement feedback loops to collect user feedback, identify issues early, and make data-driven decisions for improvement.
- **Collaboration and Communication:** Foster a culture of collaboration and open communication among development, operations, and other stakeholders. Encourage cross-functional teams, regular meetings, and shared knowledge to ensure everyone is aligned and aware of upcoming changes. All of this includes QA and QA resources.
- **Risk Assessment and Testing:** Conduct thorough risk assessments and perform automated and manual testing to validate changes before they are deployed to production. Test environments should closely resemble production to catch any issues early.
- **Change Rollbacks and Backout Plans:** Have a plan in place for rolling back changes if they introduce unforeseen issues. Document backout procedures and communicate them to the team to minimize downtime and mitigate risks.
- **Continuous Learning and Improvement:** Embrace a culture of continuous learning and improvement. Conduct post-implementation reviews (PIRs) to evaluate the effectiveness of changes and identify areas for improvement in the change management process itself.
- **Documentation and Knowledge Sharing:** Document processes, configurations, and procedures to ensure knowledge is shared effectively. Maintain up-to-date documentation that helps in onboarding new team members and enables smoother collaboration.

A final consideration is associated with the increasing number of digital solutions classified as Software as a Medical Device (SaMD). In the IMDRF document *Software as a Medical Device (SaMD): Application of Quality Management System*, it includes "There should be processes that manage risk arising from changes to system, environment, and data." This points to the

need for clear communications and change planning between application/device owners and the resources responsible for providing hosting services.

Change management in DevOps is about balancing speed and stability. By implementing these practices, the regulated company should be able to foster a culture of agility, collaboration, and innovation while managing changes effectively.

5. Glossary

TERM	DEFINITION
Application capabilities type	(ISO) Cloud capabilities type in which the cloud service customer can use the cloud service provider's applications.
Assessment	Assessment is the action of assessing someone or something.
Availability	(ISO) Property of being accessible and usable upon demand by an authorized entity.
Audit	Audit (FDA)(IEEE): An independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, or other criteria. See: functional configuration audit, physical configuration audit
CI	Configuration Item
Cloud application portability	(ISO) Ability to migrate an application from one cloud service to another cloud service
Cloud Auditor	Cloud Auditor (ISO): Cloud service partner with the responsibility to conduct an audit of the provision and use of cloud services.
Cloud capabilities type	(ISO) Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used.
Cloud computing	(ISO) Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. (CNSSI 4009-2015) A model for enabling ubiquitous, 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.
Cloud Service	(ISO) One or more capabilities offered via cloud computing invoked using a defined.
Cloud Service Broker	Cloud Service Broker (ISO): Cloud service partner that negotiates relationships between cloud service customers and cloud service providers.
Cloud Service Category	(ISO) Group of cloud services that possess some common set of qualities. NOTE – A cloud service category can include capabilities from one or more cloud capability types
Cloud Service Customers	Cloud Service Customer (ISO): Party which is in a business relationship for the purpose of using cloud services.
Cloud Service Customer data	(ISO) Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service. NOTE 1 – An example of legal controls is copyright. NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.
Cloud Service derived data	(ISO) Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer. NOTE – Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.
Cloud Service Partner	(ISO) Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.
Cloud Service Provider	Cloud Service Provider (ISO): Party which makes cloud services available.
Cloud Service Provider data	(ISO) Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider.
Commercial-Off-The-Shelf (COTS)	Is a term used to describe the purchase of packaged solutions which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.
Compute as a Service (CompaaS)	(ISO) Cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software. NOTE – To run some software, capabilities other than processing resources may be needed.
Community Cloud	Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.
Confidentiality	(ISO) Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
data portability	(ISO) Ability to easily transfer data from one system to another without being required to re-enter data. NOTE – It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy".
Data Storage as a Service (DSaaS)	(ISO) Cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities. NOTE – DSaaS can provide any of the three cloud capability types.
ECs	Ethics Committees

TERM	DEFINITION
GxP	GxP is a general abbreviation for the "good practice" quality guidelines and regulations. The "x" stands for the various fields, e.g. <ul style="list-style-type: none"> • Good clinical practice, or GCP • Good distribution practice, or GDP • Good laboratory practice, or GLP • Good manufacturing practice, or GMP
High availability	(NIST) A failover feature to ensure availability during device or component interruptions.
Hybrid Cloud	(ISO) Cloud deployment model using at least two different cloud deployment models.
IaaS	Infrastructure as a Service (NIST). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Information Security	(ISO) Preservation of confidentiality, integrity and availability of information. NOTE – In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Infrastructure capabilities type	(ISO) Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.
Integrity	(ISO) Property of accuracy and completeness.
IQ	Qualification, installation (FDA). Establishing confidence that process equipment and ancillary systems are compliant with appropriate codes and approved design intentions, and that manufacturer's recommendations are suitably considered.
IRBs	Institutional Review Boards.
LIMS	Laboratory information management system, a software-based information management tool for laboratories.
Multi-tenancy	(ISO) Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.
OQ	Qualification, operational (FDA). Establishing confidence that process equipment and sub-systems are capable of consistently operating within established limits and tolerances.
PaaS	Platform as a Service (NIST). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
PII	Personally Identifiable Information.
Private Cloud	(ISO) Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer.
Public Cloud	(ISO) Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider.
SaaS	Software as a Service (NIST). 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.
SDLC	Software Development Life Cycle - software life cycle (NIST, FDA). Period of time beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases denoting activities such as requirements, design, programming, testing, installation, and operation and maintenance.
Service level agreement (SLA)	Service Level Agreement (ISO): Documented agreement between the service provider and customer that identifies services and service targets.
Tenant	(ISO) One or more cloud service users sharing access to a set of physical and virtual resources.

6. References

- [1] Furht, Borko and Armando Escalante. *Handbook of Cloud Computing*. New York: Springer, 2010. Print.
- [2] ISO 17788 - Information technology – Cloud computing – Overview and vocabulary, 2014-10-15
- [3] The NIST Definition of Cloud Computing, Special Publication 800-145, September 2011
- [4] US Food and Drug Administration (FDA). Glossary of Computer System Software Development Terminology (8/95)
- [5] US Food and Drug Administration (FDA). Guidance for Industry: Computerized Systems Used in Clinical Investigations, May 2007

Changes from previous version

- Minor update of section 1 to reflect paper.
- Minor change to chapter 2 to reflect the purpose of the working group.
- Second question in section 3.1.2 updated partly.
- Table in section 3.2.2.2. restructured and updated.
- New section 4.2 including subsections.