Paper TT03

An Update from the PhUSE Working Group on Cloud Adoption in the Regulated Life Science Industry

Tony Hewer, Medidata Solutions Inc, London, UK

1. ABSTRACT

I shall provide a brief history of the working group's activities, our membership and, importantly, our interactions with various companies across our industry and regulators in the United States and Europe. We shall also provide information on more recent updates to our core document - A Framework for the Adoption of Cloud Technology in the Life Sciences Industry - that focuses, in particular on new approaches for auditors and regulatory inspectors.

2. A BRIEF HISTORY OF OUR WORKING GROUP

Our working group was formed in mid-2013 when the PRISME (Pharmaceutical R&D Information Systems Management Executives Forum) requested PhUSE to take on an analysis of why the adoption of cloud technologies in the Life Sciences sector was slow (compared with other industries). PRISME was inherently concerned that our sector was missing out on the various benefits (see below) that *Cloud* could bring to R&D in general.

PRISME itself is an organization not geared to undertake such an analysis initiative – hence the reach-out to PhUSE. PhUSE, on the other hand, was well positioned to leverage its membership pool as well as its well-established relationship with US Food and Drug Administration (FDA) under the auspices of the Computational Sciences Symposium (CSS) that, at that time, had been successfully in place for a few years.

So, our working group was established under the Emerging Trends and Technologies stream within CSS.

3. KEY CONCEPTS AND ASPECTS OF THE CLOUD ADOPTION FRAMEWORK

3.1 REAL AND PERCEIVED ISSUES

The first endeavour of the working group back in 2013 was to identify – and quantify - the key obstacles associated with the slow adoption issue that had been flagged by PRISME. A number of brainstorming workshops were undertaken in the latter part of 2013 and early 2014 and those obstacles were encapsulated and summarised as follows:

- In a negative sense, it was NOT the technology itself!
- There was poor, general understanding of what *Cloud* actually meant compared with past technology
- There was resistance – for multiple reasons – to the likely outsourcing of technologies (and associated roles and responsibilities) to other parties especially when the supply chains associated with those other parties could become complex (when compared with legacy approaches that mostly involved *on-prem* solutions running home-grown applications and/or licensed application software
- Unlike other industries, no standards existed for technology generally with GxP-regulated domains within the Life Sciences sector
- There was general concern around the concept of service providers utilising applications that were shared by multiple customers – even though there were robust delineation mechanisms

- Above all, the Quality Systems within Life Sciences organization tended to be highly geared to the more traditional on-prem based operations described above. This was especially vivid in the domain of computer systems validation (CSV) approaches.
- And, finally, the advent of Cloud has highlighted core underlying issues that have existed for a long time – mostly in the areas of information confidentiality and privacy controls, information security more generally as well as the utilization of information technology in a truly internationalised manner.

In reading this paper, I ask you, for now, to park these obstacles thoughts and reflect upon them in the context of the following sections.

They were initially shared with the CSS conference that took place in Silver Spring, MD in March 2014 and huge interest, discussion and engagement from attendees (both PhUSE and FDA) was generated. Moreover, it was at that conference that the idea of a *Framework* was conceived.

So, in essence, the Framework (the subject of this paper) would address the obstacles described above and, further, would propose new models of thinking that would allow the obstacles to be overcome.

Comparing then and now is interesting. Cloud technology in itself has matured and developed rapidly and in many different ways. We have observed greater adoption of cloud technology. And, we see many organizations adapting and developing their practices, Quality Systems, organizations, supply chains etc to take advantage of the benefits of Cloud.

We also observe, however, a continuation of the obstacles/issues described above. In some ways, this is to be expected; many organizations have large legacy technology investments tied up in older systems and it is likely to be many years before such systems naturally attain "retirement" modes. On the other hand, reduction of fixed costs, cost in general and improvements in overall efficiency and value are increasingly viewed as paramount across the Life Sciences sector. So, perhaps, continued cloud adoption – and the benefits of such – will accelerate such retirements.

Looking to 2014 again, back then FDA announced that they would be formulating Guidance for Industry around Cloud. The working group had a number of meetings with FDA personnel about this and FDA found those discussions valuable – including, in particular, the ideas that were going into our Framework.

Later that same year, however, FDA abandoned work on the Guidance. More recently, there has been passing reference to Cloud within, for example, guidance material associated with data integrity – not just from FDA but, also, from other regulatory bodies. This stance is to be welcomed; the focus should be on regulatory requirements and outcomes and not on the technology detail.

3.2 TECHNOLOGY EVOLUTION

In this paper, we shall dispense with any depth discussion of this topic. Suffice it to say that so-called cloud technology is, as described in our Framework, a word of jargon that's been attached to technology of recent times. That technology embraces advances in hardware and software and, above all, the "power" of the internet.

3.3 FRAMEWORK TENETS

Our Framework has a number of key tenets or design concepts as follows:

- Unlike many guidance-like documents that are published and updated very rarely, our Framework document is more of a "living" entity. It is updated on an ongoing basis by the members of the working group and made available in the public domain.
- Whilst the Framework inevitably builds upon the capabilities of today's technologies and past traditions and practices within the Life Sciences industry, it attempts to be agnostic in terms of such technology. In particular, it challenges the traditions built up in the past couple of decades that arose of the technologies of those times. Our key proposition therefore is that approaches to be taken should avoid being tied to specific technologies. Especially because those technologies will continue to develop and evolve – rapidly!

- We have avoided re-inventing terms! Hence, we have deliberately adopted terms and standards from NIST and ISO, both of which are not specific to Life Sciences.
- And, finally, we very much gear the Framework to the objective of helping stakeholders to have awareness of and, as appropriate, to conform the GxP predicate rules. In addition we demonstrate cognizance of emerging regulatory guidance associated with data integrity, transparency as well as regulations associated with information confidentiality and privacy.

3.4 A STYLIZED EDC/CTMS SETUP – THE TECH-STACK AND THE ROLES

We use this GCP-area case example to demonstrate the various permutations that can exist across different cloud technology solutions.

It is a domain that includes ***customers*** – typically pharmaceutical clinical trial sponsors, **brokers** – often shaped as Clinical Research Organizations (CROs) – and **providers** – in the form of Software as a Service (SaaS) providers supported (down the tech stack) by Paltform as a Service (PaaS) and Infrastructure as a Service (IaaS) providers.

Let's look at the ISO defintions of these players:

- Cloud Service **Customer:** In the context of GxP, these are generally the organizations or entities that purchase/use the cloud services to support their GxP-regulated activities. They 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.
- Cloud Service **Provider**: Organizations or entities responsible for providing cloud services to customers. 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 apps, infrastructure and associated service layers.
- Cloud Service **Broker**: These are the organizations or entities that manage the configuration, delivery and use of cloud services on behalf of the cloud customer. For example, cloud managers may perform infrastructure change control activities on the infrastructure built using general purpose, commercial cloud services.
- Cloud **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.

The final entity is, understandably and by its very nature, somewhat detached from the others.

The key thrust of our Framework is that the contractual and commercial interactions between these players have numerous permutations in terms of roles and responsibilities. And that this, in turn, leads to the need for clarity – a key factor in explaining things to regulators (who are, in essence, a form of ***auditor***.

Our accompanying presentation slides describe this in more detail.

4 POTENTIAL BENEFITS

There has been much written, discussed and refined on this particular topic. The high-level benefits associated with:

- The use of automated scalability coupled with payment on an usage model – leading to reduction in fixed costs
- Embedded fault tolerance
- Intrinsic high availability
- High levels of commoditization of computing, data storage and networking
- Enhanced speed of deployment
- High levels of monitoring and measurability.

No matter what we extol within our Framework, it is the Cloud Service Customer that has to make these potential benefits a reality. The business pressures to do so are compelling.

5. CONCLUSIONS

Cloud based technology solutions are here to stay!

There are adoptable ways and means for making these technologies work effectively within the regulated Life Sciences industry.

Education and awareness are key – for customers, providers and regulators.

The jargon, terminology and treatises will change into new eras of technology evolution.

Legacies will persist.

But, above all, innovations through adoption of cloud technologies are to be encouraged from within customer organizations BEFORE the demands from the business units compel things to happen.

So, a final "checklist" that summarises what can be got from our Framework and what the approach should be to embarking upon a cloud journey:

- Understand *Cloud*; it can be complex!
- Understand options and limitations
- Examine your QS and understand its limitations – and what may need to change
    - Adequacy/appropriateness of policies and procedures
    - Qualification/validation
    - Supplier management.

6. RECOMMENDED READING

Cloud Services – A Framework for Adoption in the Regulated Life Sciences Industry: https://s3-us-west-2.amazonaws.com/phuse/public/PhUSE+Cloud+Doc+13-Nov-2015.pdf

This document is also appended to this paper.

7. CONTACT INFORMATION

Your comments and questions are valued and encouraged. Please contact the principal member of the working group:

Dan Dziadiw	Merck	daniel.dziadiw@merck.com
Tony Hewer	Medidata Solutions	thewer@mdsol.com
Suzanne Studinger	QA Studinger	suzanne.studinger@qa-s.ch
Bill Telford	Sanofi	William.Telford@sanofi.com
Anders Vidstrup	NNIT	AVID@nnit.com
Chris Whalley	Amazon Web Services	whalley@amazon.com

Cloud Services

A Framework for Adoption in the Regulated Life Sciences Industry

Last Update: 13-Nov-2015

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) and/or thewer@mdsol.com (Tony Hewer, Medidata Solutions Inc.).

Pharmaceutical User Software Exchange
Cloud Adoption Working Group

Table of Contents

1 Acknowledgements

There have been eight principal authors of this document 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 paper by way of review, case studies and general discussions.

A full list of all authors and contributors will be provided here in due course.

2 Background/Introduction

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, 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.

In 2013, 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. From 2013, this working group has operated under the auspices of the Pharmaceutical User Software Exchange (PhUSE) and its collaboration with the FDA (viz., the Computational Sciences Symposium).

This PhUSE working group, comprised of volunteers from pharmaceutical industry, consultants, and Cloud Service Providers around the globe, began developing material for this framework document by identifying some key obstacles to the adoption of cloud services in GxP-regulated life sciences.

Through regular discussions and brainstorming it was recognized that different experiences of members of the working group had perspectives on technology and GxP-factors that were barriers to cloud service adoption and, further, it was surmised that if this was true in a relatively small team then industry as a whole must be having similar experiences.

With that recognition, the group began to focus on three fundamental questions that would allow each member of the group to contribute from their own experiences while learning from the experience of others both inside and outside the group:

- What are the key concepts and different varieties of cloud services available to GxP regulated organizations?
- What are the benefits and risks of the different types of cloud services in the context of GxP-regulated organizations?
- Which GxP requirements are applicable to cloud-based solutions?

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 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 document 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 controls.

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 document outlines these approaches leveraging well-recognized concepts such as the System Development Life Cycle, the Validation Master Plan as well as Coding and Deployment Standards. 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 (and that this will inexorably continue), the fundamental axioms associated with regulatory predicate rules and good engineering practices still, very much, apply and can be fully exploited.

4 Cloud Services – An Introduction

The cloud, simply, refers to software and various IT services that run on the Internet instead of on a local computer, data center, or company network. 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.

The use of cloud services is likely to have far-reaching effects on organizations in academia, industry, and government, and the cloud services industry is evolving and changing rapidly from 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[i], 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[ii] 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."*

4.1 Essential Characteristics of Cloud Services

In the context of adopting cloud for GxP workloads, understanding the essential characteristics of cloud services and solutions is important for determining the applicability of GxP requirements for specific cloud service providers and/or cloud-based solutions.

1. **On-demand self-service:** The ability to provision IT resources without requiring human interaction is a fundamentally new paradigm for life science organizations. Traditionally, GxP system provisioning has required engagement from internal departments and/or external suppliers in order to deploy computing, storage, network, and software resources. Often, these resources were manually provisioned and tested on a case-by-case basis, requiring considerable effort and coordination across multiple stakeholders while delivery of the system often lagged behind demand. In contrast, cloud-based systems can provide the capability to signup, build, test, operate, and decommission their IT resources on demand – and, often, automatically (see rapid elasticity below). In the cloud industry today, the cloud self-service model is increasingly augmented with managed services in which the cloud provider, or a third party manager, performs GxP activities on behalf of the consumer.

2. **Broad network access.** Although GxP systems have a history of being accessible from a variety of platforms and client types, cloud services is greatly expanding the accessibility of GxP systems by inherently supporting the use of networks, including the Internet, and standard mechanisms to promote heterogeneous use on thin and thick clients (e.g. mobile phones, tablets, laptops, workstations). For example, adding cross-platform support to a GxP file sharing application has

traditionally required specialized and often redundant effort for each platform, yet now with cloud services that use common web services and APIs across platforms the level of effort to achieve these cross-platform capabilities can be significantly reduced.

3. **Resource pooling.** Perhaps no other characteristic of cloud services has as much impact to interpreting GxP requirements as resource pooling. In the past, GxP users have had to purchase, commission, and manage every aspect of their IT resources, and there is a long-standing industry tradition of segregating GxP assets from non-GxP assets. Through this segregation, a lack of recognized GxP-equivalent IT standards and other factors, a paradigm has evolved where GxP practices and good IT practices are not always aligned and thus the idea of pooling and sharing IT resources across GxP and non GxP users represents new territory both from a quality assurance and compliance perspective.

4. **Rapid elasticity.** In addition to the characteristic of being on demand self-service, cloud services can also provide GxP users with new capabilities to dynamically provision and scale resources according to demand. Once the demand no longer requires a specific resource, users, automation, or a combination of the two can release and terminate the resource until they are required again. This form of rapid commissioning and decommissioning of resources holds potential to reduce variability and level of effort in qualification/validation provided the GxP consumer established the appropriate controls.

5. **Measured service.** Within GxP organizations today, IT resources are usually procured/managed as disparate services in which utilization is estimated or unmonitored altogether. In cloud services, the monitoring, control, and reporting capabilities can provide increased transparency, auditability, and cost controls.

4.2 Cloud Service Models in the Traditional GxP Computerized System Context

In good Laboratory, Clinical, Manufacturing and Distribution practices (GxP), 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".[iii]

With such a *traditional* computerized system, a GxP-regulated organization (hereinafter referred to as the "GxP Owner") develops a laboratory, clinical, or manufacturing process that may benefit from the use of computers for recordkeeping and data collection.

When organizations have established IT policies and standards, the GxP Owner purchases and installs the physical hardware, infrastructure software (operating system, database environment, application stack, etc.) and a GxP Application. When these computerized system components are installed in the GxP Owner's 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" which are considered lower risk by the GxP Organization. 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 Owner 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, the GxP Owner's interpretation of applicable requirements, and supplier assessment(s). GxP applications are installed on the qualified infrastructure, configured for the specific GxP processes and procedures, and then tested to ensure the GxP Owner's intended use 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").

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	*GLP/GCP/GMP 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).

4.2.1 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. [iv] When IaaS is incorporated into GxP computerized systems, Cloud Service Customers retain a number of GxP responsibilities ensuring the qualification status of this infrastructure.

Cloud Provider	GxP Consumer	GxP Requirements
	GxP Organization	*Cloud Policies & Standards*
	GxP Intended Use	*SOPs/Process Validation*
	Software	*Software Operations* *Software Validation* *Software Procurement/Development*
	Platform	*Infrastructure Maintenance* *Infrastructure Qualification*
	Infrastructure Resources*	
Cloud Infrastructure		*Service Level/Quality Agreement* *Supplier Assessment*

Figure 2 – GxP responsibilities ensuring the qualification status of Infrastructure as a Service

4.2.2 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.

Cloud Provider	GxP Consumer	GxP Requirements
	GxP Organization	*Cloud Policies & Standards*
	GxP Intended Use	*SOPs/Process Validation*
	Software	*Software Operations* *Software Validation* *Software Procurement/Development*
Platform		*Service Level/Quality Agreement* *Supplier Assessment*
Infrastructure Resources		

Cloud Infrastructure		

Figure 3 – GxP responsibilities ensuring the qualification status of Platform as a Service

4.2.3 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.

Cloud Provider	GxP Consumer	GxP Requirements
	GxP Organization	*Cloud Policies & Standards*
	GxP Intended Use	*SOPs/Process Validation*
Software		*Service Level/Quality Agreement* *Supplier Assessment*
Platform		
Infrastructure Resources		
Cloud Infrastructure		

Figure 4 – GxP responsibilities ensuring the qualification status of Software as a Service

4.3 IT Supply Chain in the Cloud Era

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.

4.3.1 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 just a few of the basic roles based, here, on NIST.

- **Consumer:** 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. [The associated ISO term is Cloud Service Customer.]

- **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. [The associated ISO term is Cloud Service Provider.]
- **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. [The associated ISO term is Cloud Service Brokers.]
- **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. [The associated ISO term is Cloud Auditor.]

4.3.2 Activities and Examples in the Cloud Supply Chain

In this document, 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.

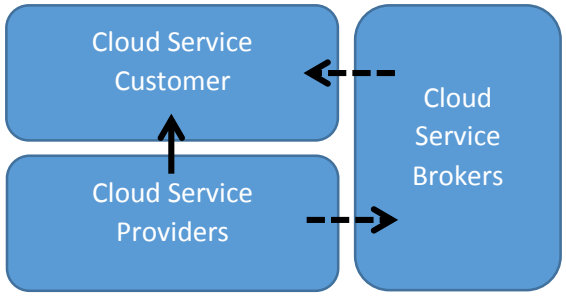

Figure 5 – Connection between roles/parties in usage/provision of cloud services

Hence, the following, more 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".

	IaaS	PaaS	SaaS

Cloud Service Customer	Manages privileged and/or service accounts Defines and manages workflows supporting application needs Conducts additional qualification of infrastructure according to intended use	Manages privileged accounts and/or service accounts. Defines and manages workflow supporting application needs Conducts additional qualification of infrastructure- and platform according to intended use	Manages user accounts and roles Defines and manages workflow supporting application needs Conducts validation of applications according to intended use
Cloud Service Broker	Defines service requirements based on the approved service business case and the service risk assessment. Assesses service risk. Selects Cloud Service Provider on behalf of or together with the Cloud Service Customer.	Describes service, including service level options. Describes the architecture. Defines cloud service provider KPIs. Identifies relevant CIs based on the service risk assessment. Evaluates the need for standards for the service on behalf of or together with the Cloud Service Customer.	Releases service. Ensures implementation of services by the Cloud Service Providers according to the defined service requirements and agreed service levels.
Cloud Service Providers	Provisions and manages the physical resources, builds and maintains the resource abstraction and control layer. Provides Customer Support. Provides handling of security and risk identifications and controls. Qualifies Infrastructure services.	Implements and/or deploys services according to the defined service requirements and agreed service levels. Operates services. Provides Customer Support. Provides handling of security and risk identifications and controls. Qualifies Infrastructure- and Platform services	Implements or deploys services according to the defined service requirements and agreed service levels. Operates services. Provides Customer Support. Provides handling of security and risk identifications and controls. Validates generic functionality in application

5 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 that are impacted by the cloud technology. 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 vetted in these key control areas. The extent of this vetting needs to approach - or exceed - the level of assurance related to their own IT systems within their own data centers (for example). The following describes the major areas where such vetting is crucial to establishing this assurance.

5.1 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, thru 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.*'

Some of the most crucial aspects of the vetting 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 later in this document, with their own separate sections.

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 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
- Change management
- Problem Management
- Incident management
- Identity and Access management
- Back-up and restore
- Business Continuity and Disaster Recovery.

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 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. With that said, creation of a prescriptive Cloud Service Customer cloud-specific guidance is also recommended to support the specifics of a Cloud Service Customer's SDLC policy, as well as their overall cloud-adoption process. 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 compliance team's 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, it has become an expectation that Cloud Service Customer of cloud services will be able to demonstrate that the infrastructure and/or underlying platforms are qualified. This is to ensure that the underlying components that support core-business applications are standardized and reliable. This Qualification strategy is often defined as part, or a subset, of the overall SDLC policy. As such, this qualification strategy is often a reduced set of deliverables that is required for business applications or services and often includes the following:

- Quality Assurance/Qualification Plan, Requirements and Design/Configuration Specifications (e.g. Technical Standards, Degree of customization required, Parameter settings)
- Infrastructure IQ/OQ (Installation/functional qualification)
- Formal Agreements (e.g. Service Level Agreements (SLAs)/Operating Level Agreements (OLAs))
- SOPS governing specific Infrastructure/Platform processes
- SOPs governing Infrastructure's approach to the support of GxP applications
- Manuals/Work Instructions/Knowledge Management
- Disaster Recovery and/or Business Continuity Plans for critical services/infrastructure utilities.

As noted previously, much of this information may reside with the Cloud Service Provider or Cloud Service Broker. Therefore Cloud Service Customers will need 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.

5.2 Supplier Management Policies

Cloud service models are unique in that they typically involve external IT Suppliers 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. This is unlike a software vendor that may provide a product, but where the Cloud Service Customer takes fully ownership after the purchase. Therefore, key policies around management of these types of cloud suppliers become paramount.

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 especially 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, much of the overall cloud offering is supported by third parties. 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 Brokers and the Cloud Service Provider 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. Section 7.2 provides more details on agreement contents.

Supplier 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 available upon request, as this is an expectation of regulatory agencies for all systems supporting regulated business functions. Because Cloud Service Brokers and Cloud Service Providers provide both services and systems to provide those services, the overall assessment process will require an in-depth analysis of both. As such, the detailed 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.

5.3 Information Risk Management, Privacy and Data Protection Policies

Overall 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 Provider's risks. Output of such assessment may include high-risk findings that need to be treated and 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, or the possibilities of where this type of information may be stored geographically as this impacts 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.

5.4 Cloud 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.

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 more aligned to the requirement artifacts created as part of the SDLC process - to ensure key security considerations are incorporated as part of the implementation of the system. This may include both technical controls required for the implementation (i.e., authentication methods), 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. In general, many of these control requirements are typical and consistent with other types of non-cloud technology implementations.

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 following includes key core elements of security that should be vetted with the Cloud Service Provider;

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 Internet region 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:

- 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
- 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.

Please refer to NIST[v]

6 Glossary

ECs	Ethics Committees
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).
IQ	Qualification, installation. 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
OQ	Qualification, operational. 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.
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.

7 Appendices

7.1 Quality Responsibilities Matrix

7.1.1 Buildings and Facilities

			Responsibility		
	Requirements	**Records** **(Select all that apply)**	**N/A**	**GxP Owner**	**Supplier**
	Buildings should be designed, constructed, and located to facilitate cleaning, maintenance, and proper operations.	☐ Building site risk assessment ☐ Facility capacity requirements ☐ Redlined or as-built facility drawings ☐ Facility maintenance and repair records ☐ Facility safety inspection records	□	□	□
	Utilities, environmental controls, and backup systems should be designed, installed, monitored, and calibrated as appropriate for the data center and services.	☐ Utility hookup and verification records ☐ Calibration and monitoring records for environmental monitoring instruments ☐ Facility backup system verification records	□	□	□
	Standard operating procedures (SOPs) and responsibilities for facility maintenance activities should be maintained and approved.	☐ Approved SOPs (including responsibilities) ☐ Training records for responsible personnel	□	□	□
	Facilities should be secured to protect against theft and tampering, and access into areas where equipment are held should be limited to authorized personnel.	☐ Approved building security plan ☐ Current list of personnel with building access ☐ Building visitor logs ☐ Security system documentation	□	□	□
	Business continuity plans should be maintained and include facility disaster response, recovery, failover.	☐ Approved business continuity plans ☐ Method for plan invocation ☐ Definition of review and update cycle	□	□	□

7.1.2 Equipment, Physical Infrastructure

	Responsibilities	Records (Select all that apply)	N/A	GxP Owner	Supplier
	Physical equipment should be of appropriate design, capacity, and location for its operation and maintenance	☐ Inventory of physical infrastructure components ☐ Verification that physical equipment requirements are met by the utilities and physical environment (power, temp, etc) ☐ Protection against damage from natural causes and disasters. ☐ Supplement of redundant equipment located at a reasonable distance.	□	□	□
	New hardware models and assemblies should be qualified in a production-like environment before being released to production.	☐ Approved test protocols demonstrating that new hardware can meet production environment requirements. ☐ Approved test reports showing that requirements are met and test deviations are resolved.	□	□	□
	Installation, maintenance, repair, and replacement responsibilities should be documented and proceduralized, including schedules and triggers for condition-based activities.	☐ Approved SOPs for equipment installation, maintenance, repair, and replacement ☐ Records for equipment maintenance, inspection, repair and replacement activities (including the name and date of the person(s) performing the activities)	□	□	□
	Identifiers for physical hardware (serial numbers, asset tags, or other ID) should be logged and traceable to virtual machine identifiers such that any problems above the hypervisor that result from hardware problems can be traced to the specific piece(s) of equipment that caused the problem.	☐ Hardware ID logs ☐ Written (or automated) procedures for correlating physical hardware IDs and virtual hardware IDs	□	□	□
	Hardware nonconformities resulting from defects in manufacturing or assembly should be reported to the manufacturer/assembler.	☐ Records of hardware nonconformity reports and communication with manufacturers	□	□	□

	Responsibilities	Records (Select all that apply)	N/A	GxP Owner	Supplier
	Hardware nonconformities resulting from defects in installation and maintenance should be corrected, logged, investigated, and prevented.	☐ Records of hardware nonconformity reporting and investigations	□	□	□
	Qualification tests should prove that the system works as designed, including I/O error handling, error verification, correction verification, and allowable error over-rides.	☐ Pre-approved I/O test protocols ☐ Completed test report showing requirements are met and test deviations are resolved	□	□	□

7.1.3 Software, Physical Infrastructure

	Responsibilities	Records (Select all that apply)	N/A	GXP Owner	Supplier
	Software manuals should be available and current with the software version(s) in production.	☐ Software manuals ☐ Release notes	□	□	□
	Approved standard operating procedures (SOPs) should be maintained for software testing, deployment, operations, and maintenance.	☐ Approved SOPs	□	□	□
	Backup of software in production should exist and be maintained in a restorable state.	☐ Backup and restore verification records.	□	□	□
	System configuration should be verified	☐			
	Devices (Firewall, IDS, SAN, etc)	☐			

7.1.4 Software, Virtualization Services

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GxP Owner	Supplier
	Software manuals should be available and current with the software version(s) in production.	☐ Software manuals ☐ Release notes	☐	☐	☐
	Approved standard operating procedures (SOPs) should be maintained for software testing, deployment, operations, and maintenance.	☐ Approved SOPs			
	Device configurations	☐			
	Operating Systems	☐ Patch management			
	Database software	☐			

7.1.5 Equipment, Virtual Infrastructure

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GxP Owner	Supplier
	Computer equipment should be of appropriate design, capacity, and location for its operation and maintenance.	☐	☐	☐	☐
	Identifiers for virtualized hardware (serial numbers, asset tags or other ID) should be logged.	☐ Hardware ID logs	☐	☐	☐
	Virtual machine logs...	☐	☐	☐	☐
	O/S log files…	☐	☐	☐	☐

7.1.6 Software, Application Platform

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GxP Owner	Supplier
	Platform software/run time environment	☐	☐	☐	☐
	Information Security Measures	☐ Vulnerability assessments ☐ Intrusion prevention/detection			

7.1.7 Software, GXP Application

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GXP Owner	Supplier
	Procedures for development, testing, release to production	☐ Change Control SOP ☐ Policy and SOPs for SW Development Lifecycle ☐ Release Notes	□	□	□
	Data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, third-party obligation for retention, and prevention of unauthorized disclosure or misuse	☐ Approved procedure for data classification assessment.	□	□	□
	Electronic Record and Signature Controls	☐ Password policy ☐ Definition of Access Levels ☐ User Administration ☐ Part 11 testing ☐ Data Classification and protection from unauthorized use, access, loss destruction and falsification ☐ Compliance with defined retention periods and end-of-life disposal requirements ☐ Segregation of keys ued for encrypted data or sessions	□	□	□
	Validation and user acceptance testing	☐ CSV policy and SOPs, incl. handling of nonconformities ☐ Performance and approval of UAT ☐ Requirements for Backup	□	□	□

7.1.8 Organizations and Personnel

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GXP Owner	Supplier
	Sufficient resources	☐ Org chart indicating responsible area managers	□	□	□
	Personnel should have the education, training, and experience to allow them to perform their assigned functions.	☐ Job descriptions ☐ Resume/CV ☐ Training records	□	□	□
	Organizations should not use in any capacity the services of any person debarred under the Generic Drug Enforcement Act.	☐ Background check records for debarment	□	□	□
	A quality or compliance unit should have the responsibility and accountability for ensuring policies and procedures are established and followed.	☐ Quality Manual	□	□	□

7.1.9 Privacy and Security

- Physical security is in buildings and facilities section
- Logical security is distributed in the appropriate software sections.

7.1.10 Quality Systems

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GXP Owner	Supplier
	Effective arrangements for customer communication should address product/service information, contracts and amendments, customer feedback and complaints, change notifications, and advisory notices.	☐ Written product/service literature and user documentation ☐ Written procedure(s) for customer complaint/issue handling and investigations ☐ Records of customer complaint investigations ☐ Written procedure(s) for issuing and implementing customer advisory notices	□	□	□
	Documented procedures should exist for reviewing nonconformities (including customer complaints), determining root cause, evaluating need for action, recording results of nonconformity investigations, and	☐ Approved SOPs for corrective actions and/or nonconformity investigations ☐ Records of nonconformity investigations (including customer	□	□	□

	Responsibilities	Auditable Artifacts (Select all that apply)	N/A	GXP Owner	Supplier
	reviewing corrective actions for effectiveness.	complaints) and the corrective actions taken (if any) ☐ Written process for reviewing effectiveness of corrective actions.			
	Documented procedures should exist for identifying potential nonconformities and their causes, evaluating need for action to prevent occurrence, and determining and implementing action needed.	☐ Approved SOPs for preventive actions ☐ Records of nonconformity trending, evaluations, and preventive actions taken (if any) ☐ Written process for reviewing effectiveness of preventive actions.	□	□	□
	Establish and maintain procedures to control documents required.	☐ Policy ☐ Procedure ☐	□	□	□
	Risk Management	☐ Approved process ☐ Assessment to include Identification of critical data and services, ☐ Identification of dependencies inc. processes, applications, business partners and third party providers ☐ Definition of maximum tolerable period of disruption of service (recovery time objectives) ☐ Regular conduction of risk assessments associated with data governance requirements considering where sensitive data is stored and transmitted across applications, servers and network infrastructure			
	Management responsibility	☐ Self inspections	□	□	□
	Purchasing controls	☐ Independent reviews and assessments at regular intervals (shared audits?)	□	□	□

7.1.11 Recordkeeping

For records under the responsibility of multiple parties the Quality Agreement needs to define the requirements for approval and retention of original records.

7.1.12 Validation and Qualification

Validation and qualification requirements are distributed throughout the above checklists.

7.2 [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.

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

- 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, Frequency).

8 References

[i] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[ii] ISO 17788 - Information technology — Cloud computing — Overview and vocabulary
[iii] Food and Drug Administration. Guidance for Industry: Computerized Systems Used in Clinical Investigations.
[iv] Furht, Borko and Armando Escalante. *Handbook of Cloud Computing*. New York: Springer, 2010. Print.
[v] http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf