CLOUD VALIDATION IN GXP ENVIRONMENT

Infosys®
Navigate your next
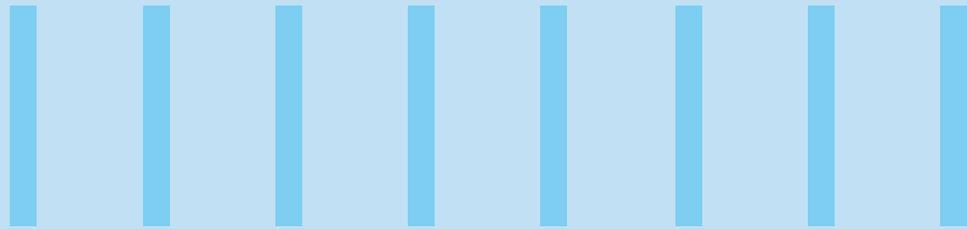
Introduction

Pharma industries are embracing cloud computing as an innovative, economic, and compliant solution to increase the collaboration of clinical trials, expedite the pharma value chain, improve patient experience, and manage costs. The migration to cloud and using cloud services should be validated. This paper covers the validation strategy for cloud migration.

Migration to Cloud

The transfer of the company's hardware and software resources from on-premises or existing cloud to another cloud is called cloud migration.

Validation of Cloud Migration (from On-Premises to Cloud or Cloud to Cloud)

Validation of cloud migration comprises of validation and migration of infrastructure, data, and applications from on-premises to cloud or cloud to cloud. Validation of cloud migration is covered in four phases:

Operations

- Operation processes – Incident ,change, SLA Monitoring, Periodic Review
- Audit & security assessment

Deploy (Infrastructure Qualification, Migration, Validation of data, application)

- Infrastructure qualification as per GAMP guidance
- Data Migration plan, specification, migration & validation scripts and report
- Application migration as per strategy
- Validation of application using CSV model

Planning

- Charter / Project plan
- Communication Plan
- Deployment Plan
- Initial Change Management
- Selection of tools
- R&R

Assessment

- Design Consideration
  - Assess inventory of computing resource (Dependencies, Complexities , Risk, Prioritization)
- Deployment Consideration
  - Decision on landing zone
  - Selection of 6 R's
- Cost estimation
- Selection and Assessment of Vendor (Contract, Proof of Concept, landing zone assessment)
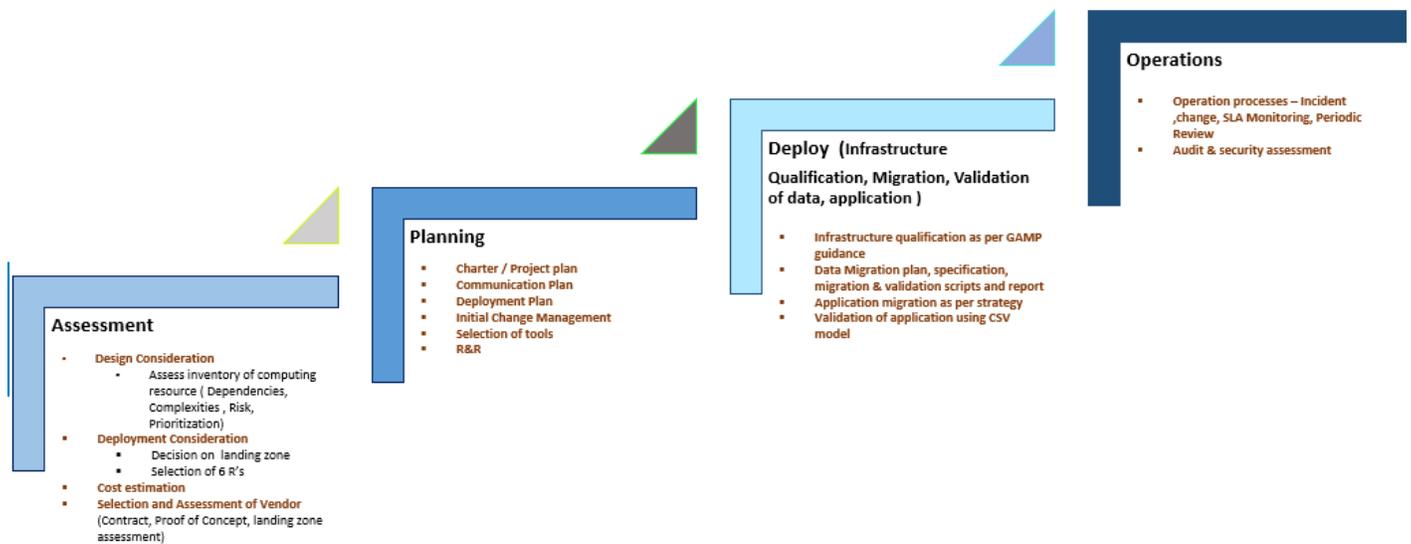
Figure 1

- **Assessment/Determine Phase:** This phase is the basis of validation of cloud migration. Appropriate research, assessment, and identification of the company's requirements are critical to making the right decision. Relevant stakeholders should be involved to assess and strategize on the following:

  o Identify and assess the inventory of on-premises computing resources such as infrastructure, applications, related components, operating systems, platform support, and any third-party tools.

    - Analyze the on-premises infrastructure in terms of size, capacity, and architecture.

    - Organize your apps into categories based on their complexity and risk. Discover the application portfolio and the associated dependencies.

    - Derive the list of infrastructure and applications ready for migration.

    - Evaluate the needs and resources such as virtual machines, application servers, storage servers, and database servers.

  o Deployment Consideration – Deployment consideration starts with identifying the requirements of the landing zone and the selection of a strategy for the migration of data and applications to be deployed. Refer to details on landing zone and 6R migration strategy for applications in appendix A.

  o Cost Analysis – This is about estimating the cost associated with applications and infrastructure migration. As we choose CSP, an assessment of the Total Cost of Ownership (TCO) should be done.

TCO analysis helps to determine and assess the total cost of ownership of the existing infrastructure and its equivalent TCO on cloud-based infrastructure.

  o Now, choose and assess the CSP. The contract should be documented and signed based on the review and confirmation of the following –

    - Certifications on applicable regulatory requirements such as ISO27001, SOC1 Type II, Web Trust, ISO 9001, NIST, HIPPA, HITRUST, COBIT, CFR Part 11, and annex 11, etc.

    - Contract should cover policy on data governance, data security, server locations, and controlled environment. Procedural, technical, and operational controls to ensure the protection and confidentiality of customer data, performance, reliability, and availability of the cloud should be in place.

    - Physical and logical security controls followed by CSP for different service models.

    - Qualification documents of the landing zone should be reviewed. Landing zone must provide network capabilities and automated facilities related to accounting management and security, backup, disaster recovery, and operation support.

    - Communication strategy on patch installation, updates to infrastructure, customization of applications, etc. must be informed and documented.

    - Roles and responsibilities related to cloud services must be defined and agreed upon.

    - In case of using infrastructure (IaaS) and platform (PaaS) service model, qualification documents of infrastructure and environments should be reviewed. In case of the SaaS model, validation deliverables of the application should be reviewed by the customer.

    - Trained resources and technologies must be in place to confirm stable business health of the cloud. Migration support to move to another arrangement (vendor lock-in) should be signed.

- **Planning Phase:** The planning phase starts post-assessment. It involves-

  o Building a skilled team, who understands and has experience with the business processes, technology, and use cases.

  o Identifying migration tools, creating a project plan, communication plan, and schedule to migrate infrastructure, data, and application.

  o Changing the management process. It must be followed to ensure traceability, documentation, and relevant approvals. Define and document groups, roles & responsibilities.

Note: Communication plays a major role in successful migrations.

- **Deployment Phase (Migration, Infrastructure Qualification, Application Validation):** Deploy phase comprises- qualification of infrastructure, migration of data (if applicable), migration, and validation of the application. The scope of work is as per client requirements.

The table below provides a qualification/validation approach for three service models -

Service Model	Qualification/Validation Approach
IaaS	• Review and confirmation of documentation of CSP's landing zone and infrastructure of cloud as per Infrastructure GAMP5 guidance • Qualification of infrastructure migrated from on-premises to the cloud. The qualification activities of components vary as per the service and function in their respective infrastructure layers • Integration of migrated infrastructure on Cloud • Migrate data (if applicable) using a data migration plan, requirements, testing, and report
PaaS	• Review and confirmation on documentation of CSP's landing zone and infrastructure of cloud as per Infrastructure GAMP5 guidance • Qualifying PAAS based on requirements and risk-based approach. It includes testing of OS, configurations, environments, libraries, etc • Migrate data (if applicable) using data migration plan, requirements, testing, and report
SaaS	• Review and confirmation of documentation of CSP's landing zone, the infrastructure of cloud, and platform as per Infrastructure GAMP5 guidance • Migrate data (if applicable) using a data migration plan, requirements, testing, and report • Review of documentations (URS, FS) of application and testing (functional, performance, any other such as security, remote connection testing) of application

Table 1

Migration and Validation Process for Data and Application

The validation of data and application migration will be done once the infrastructure and environment are qualified. The data migration process involves validated tools, documentation, testing, and approvals.

It starts with the data migration plan, requirements, and testing and completes with a data migration report. Migrated data must be validated to confirm accuracy and completeness. Once data migration is successful, application migration will start as per identified 6R strategy. Application validation will follow the 'V' model for validation. The table given below provides key deliverables needed for the specific strategy.

Migration	Validation Strategy			Key Deliverables
	Dev Env.	Quality Env.	PROD Env.	
As-Is (Re Host)	IQ	IQ OQ (Regression) Performance	IQ	• Validation Plan • IQ/OQ/PQ Strategy • IQ/OQ/PQ Reports • Validation Report
Re-Platform/Upgrade (Re-Host with Upgrade)	IQ	IQ OQ (Regression) Performance	IQ	• Validation Plan • System Specifications • IQ/OQ/PQ Strategy • IQ/OQ/PQ Reports • Validation Report
Refactor/Re-architect/ Remediate (Source Code Updates)	IQ, Unit Testing	IQ OQ Performance	IQ	• Entire validation cycle deliverables
Replace with SaaS Model	N/A	Existing Documentation	PQ	• Validation Plan • PQ includes security testing • Validation Report
Retire	N/A	N/A	N/A	N/A
Retain	N/A	N/A	N/A	N/A

Table 2

• Retain and Retire strategy has no deliverable from a cloud migration and validation perspective

• Cloud vendor assessment and data migration are common to all types of migrations

• **Operations & Optimization Phase:** Operation and optimization phase demands documentation, execution of operation processes, training, trained resource, reports, SLAs, performance, and continual improvements.
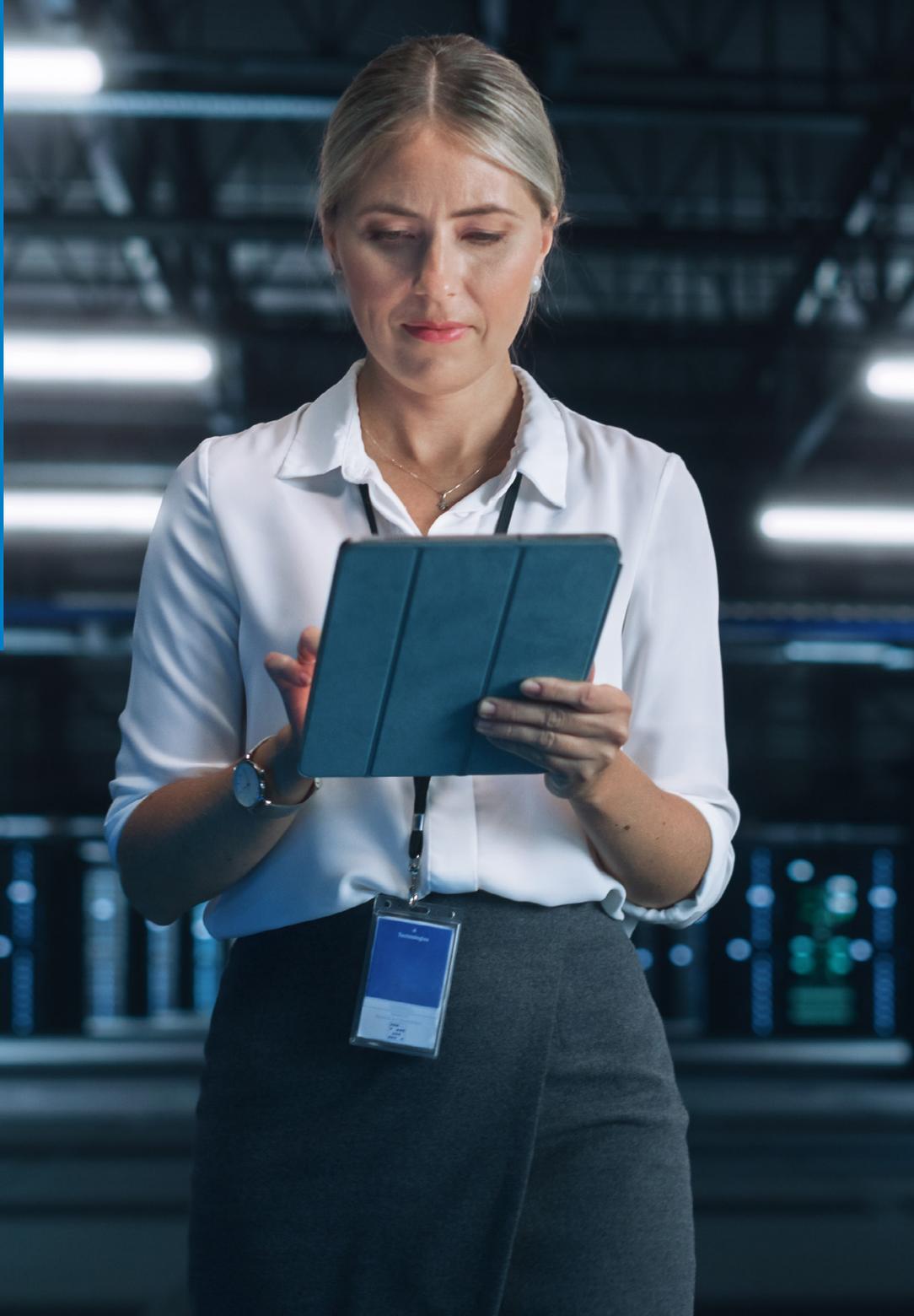
Secret of Successful Cloud Migration

Assessment and planning are the two differentiators of cloud validation. Both phases build risk-based analysis and ensure coordination and alignment. The success of cloud validation depends on complete assessment and proper planning.

Conclusion

The pharma industry needs upcoming technologies to address concerns and explore globally. All new technologies such as IoT, AI, ML, DevOps, etc. are dependent on the cloud for speed, scalability, and availability. Cloud migration is very much in demand considering the globalization, huge data, and regulatory need of the pharma industry. Usage of cloud is a long-time investment to earn profits in the future. This highlights the importance and demand of cloud validation consultants who ensures compliant cloud.

References

- https://ispe.org/publications/papers/leveraging-paas-regulated-environment

- https://ispe.org/pharmaceutical-engineering/september-october-2014/challenges-regulated-life-sciences-companies

- https://www.cloudflare.com/learning/cloud/what-is-cloud-migration/

- https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

- https://www.cloudflare.com/learning/cloud/

Appendix A

Cloud Deployment Model

Private	Community	Public	Hybrid
Cloud infrastructure is dedicated to only one organization. It may or may not be on-premise or managed by an organization. E.g.: • HP Data Centers	Cloud infrastructure is provided as a service to a specific community of consumers with common interests and concerns such as security and compliance. E.g.: • IBM Smart Cloud • Google App Engine • Amazon EC2	In this model, cloud infrastructure services are open for public use. Most of the time, the public cloud is owned, managed, and operated by a cloud service provider. Multiple tenants are renting and using the same server space (Multitenancy) E.g.: • Amazon Elastic • Google App Engine	This model can be a combination of any other models (private, community, or public). Model enables porting of data and load balancing of application between clouds. E.g.: Google cloud

Cloud Service Models – Cloud Service models are built on a shared-responsibility approach between Cloud Service Provider (CSP) and consumer/client.

Infrastructure-as-a-Service (IaaS)	Platform-as-a-Service (PaaS)	Software-as-a-Service (SaaS)
Infrastructure resource is provided to the consumers as per their requirements. The resource includes network, compute resources, etc. Consumers can utilize these resources for the deployment of operating systems, environments, and the development of applications. The cloud infrastructure is not controlled or managed by consumers. However, the consumer has defined and less control over networking components. (E.g.: firewalls)	This model provides infrastructure as well as a platform (operating system, run-time environments, libraries, tools) to consumers to develop/deploy applications. Infrastructure, as well as platform, is managed by a cloud service provider.	Consumer is provisioned with infrastructure, platform, and applications. Applications are accessed through a thin client interface such as a web browser. Consumer does not control and operate cloud infrastructure, platforms, or applications. The consumer can ask for configuration settings, limited to a certain level.

6R Application Migration Strategy

Rehosting (lift-and-shift)	Re-Platforming	Re-architecting/ Refactoring	Repurchasing/- Replacing	Retain	Retire
The application will be as it is copied to the cloud environment. Relatively low migration effort. Migration speed is good. Migration tools can be used to rehost.	In this strategy, the architecture of the application will not change. But there will be changes adopted as per the cloud platform for optimization. E.g. PaaS database replace the application database.	Usually applies to critical and outdated applications. The code of the application will be updated. Need high migration effort. Re-architecting help in utilizing optimization of the cloud.	SaaS solution will replace the legacy application.	The legacy application is retained. In such cases, application and application data may be of high priority and secure. The application is under the control of the client.	Application is not needed, hence retired.

Landing Zone

The landing zone is a pre-configured environment with a standardized set of secure cloud infrastructure best practices, guidelines, policies, and centrally managed services.

About the Author

Pooja Mishra

Pooja has experience in validation of application, Infrastructure Qualification and Cloud Validation, in scope of roles - validation manager, quality lead etc. She has experience in internal audits and periodic reviews as well.

For more information, contact askus@infosys.com

Infosys
®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected