KPMG

GxP compliance in cloud infrastructure

Aug 2022

home.kpmg/in

In this era of digital transformation, where artificial intelligence, virtual and augmented reality have garnered attention, cloud computing is proving to be the enabler for these technologies. Pharmaceutical, medical devices and biotech companies are increasingly exploring digital solutions to improve their drug development processes, supply chain, research, manufacturing of medicines and devices etc.

Cloud infrastructure is based on a shared responsibility model, which eases the technical responsibilities of an organisation. The cost-effective pay-as-you-go solutions, computing scalability, advanced analytics and automation capability provided by cloud give an edge over on-premises infrastructure.

Along with cloud, colocation data centres are also garnering interest since the providers permit customers to use their own hardware and configuration that meets their evolving requirements.

While these services have enamored other industries, for life sciences industry, the uptake has been a little slower in comparison. This paper explores a phased approach to implement GxP compliance in cloud infrastructure and colocation facilities. Areas that require attention and need due diligence, to meet the regulatory requirements have been highlighted.

1. Regulatory changes

As organisations are looking to implement next-generation technologies including cloud, the regulatory bodies are optimistic about ensuring compliance and data integrity. Agencies like US FDA, EMA and MHRA are shifting focus to accelerate innovation and support the use of automation and emerging technologies in the designing and manufacturing of drugs and medical devices.

FDA is publishing a new draft guidance—Computer Software Assurance (CSA) for Manufacturing, Operations and Quality System Software. These guidelines are expected to address existing barriers to technology adoption and encourages the use of automation tools and underlying IT solutions.

CSA attempts to shift focus to a critical thinking approach and is a green signal to encourage the use of automation and digitisation solutions, agile testing methods (unscripted testing and ad hoc testing) and leveraging vendor documentation. This approach would help shift companies' focus area from rigid compliance measures to developing and sustaining a culture of innovation, implementation and adherence

2. Phased approach for cloud adoption

Onboarding the cloud infrastructure requires a phase wise approach to ensure that all risks are considered, mitigation controls are implemented and required evidence is documented for a smooth and compliant movement to the cloud landscape.

Concept phase

During initial stages, regulated organisations should assess benefits of bringing in cloud solutions by weighing the risk and impact.

Typical deliverables - Quality Management System (Policies, Procedures, Templates), Training Records, Change Control, Vendor evaluation report

- Raise change control. Consider the following:
  - High level risk
  - Rollback plan
  - Compliance documentation
  - Timelines
- Revamp Quality Management System to include approach for moving to cloud-based IT Infrastructure and solutions
- Select personnel with adequate experience
- Perform vendor evaluation based on (but not limited to) the following parameters:
  - Market size and relevant experience
  - Performance history
  - System development life cycle practices
  - Quality management system
  - Available documentation
  - Testing practices
  - Data integrity practices
  - Business continuity/disaster recovery
  - Defect management
  - Support and maintenance services
  - Personnel trainings
  - Third party management.

Planning phase

Moving to cloud requires active planning and defining a clear strategy. Onboarding the right implementation partner with skillset in technical and regulatory aspect of cloud is essential

Typical deliverables - Impact assessment, Project Plans, Qualification Plans

- Understand security strategy (capability gap assessment, roadmap, business case)
- Perform quality and regulatory assessment. Consider the following:
  - GxP impact
  - System classification
  - ER/ES assessment (as applicable)
- Qualification strategy:
  - Scope definition and responsibilities
  - Lifecycle activities
  - Deliverables and approvals
  - Constraints and prerequisites
  - Cloud security and compliance activities
  - Overview of the planned architecture
  - Training requirements.
- Consider share of responsibilities-

Responsibilities / Models/ Services	Customer Responsibility	Cloud Provider Responsibility
Software as a Service	• Data access policies • End Devices • User identities	• Applications • Network Access • Operating System • Network Infrastructure • Datacentre • Physical Host • System Patches
Platform as a Service	• Data access policies • End Devices • User identities • Applications	• Network Access • Physical Host • Network Infrastructure • Datacentre • Operating System • System Patches
Infrastructure as a Service	• Data access policies • End Devices • User identities • Network Access • System Patches • Applications • Operating System	• Physical Host • Network Infrastructure • Datacentre • System Patches
On premise	• Data access policies • End Devices • User identities • Applications • Network Infrastructure • Datacentre • Operating System • Network Access • Physical Host • System Patches	

Risk management phase

During the risk management phase, GxP impact and associated risks are to be identified and mitigated through a controlled and secure architecture. SLAs are to be defined and verified during validation testing of the cloud infrastructure.

Typical deliverables - Infrastructure risk assessment, Test plans.

- For the key risk areas, identify the required mitigation controls
- Assess severity, predictability and detectability of risks
- Identify SLAs to reduce risks of shared responsibilities based on (but not limited to) -
  - Responsibilities
  - Up time / Down time
  - Backup and recovery
  - Security
  - Data Storage Location
  - Performance Monitoring
  - Service Termination
  - Compliance management
- Assess cloud security programme risks:
  - Information and Privacy Protection
  - Identity and Access Management
  - Incident and Crisis Management
  - Threat and Vulnerability
- Identify mitigation actions to reduce risks for technical controls
- Consider design requirements and update/ make changes to design specification
- Define scope of testing needed based on risk identified
- Create test plan.

Specification and Design phase

Based on the risk identified, the architecture of the cloud infrastructure should be assessed and specifications to be documented based on the components selected. The deployment model should consider all the security risks, procedural and technical controls needed and continuous monitoring mechanisms.

Typical deliverables - Infrastructure requirements specification, Design specification

- Specify controls and responsibilities based on the service/platform models
  - Personnel and SOD controls
  - Controls to manage risks and adhere to regulations
  - Specify service models to fulfil the business operations
  - Platform components - Clients/Applications.
- Design high-level cloud architecture for all the relevant source of requirements, Data Management, Platform Backup, and storage design
- Specify deployment models
- Secure deployment approach
- Specify and design end-to-end security, risk and compliance framework:
  - Design security controls
  - Specify and manage risks
  - Design compliance aspects
  - Specify configurations.
- Design and integrate cloud-native controls and configure policies for each service
  - Integrate and configure cloud native controls
  - Policies and procedures
  - Specify SLA with cloud platform provider.
- Define procedural / technical controls for the following GxP areas-
  - User identity and access management
  - Audit trails
  - Data integrity
  - Network security
  - High availability
  - Backup restoration
  - Business continuity management
  - Performance monitoring
  - Incident management
  - Change control and configuration
  - Archiving and retrieval
- Define data migration activities and requirements (if applicable)

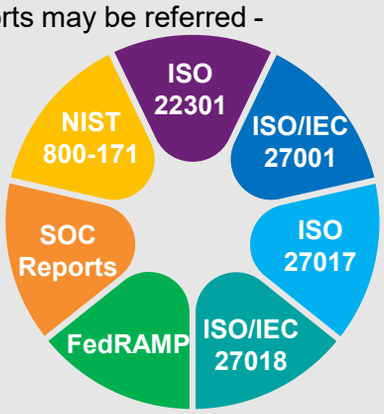
- Define automated cloud monitoring mechanism:
  - Set up user access and health check-up logs
  - Define events and set a detect mechanism
  - Build alerts triggered based on events
  - Set mechanism to notify the administrative group.

Testing phase

To provide assurance, testing needs to be performed against the specifications. In a cloud landscape, it is not possible to verify some of the vendor managed infrastructure components. Existing certification and audit reports provided by the cloud service providers need to be referred and availability of adequate controls to be verified.

Typical deliverables- Qualification protocols, Test reporting, Traceability

- Author and execute qualification protocols
- Verify if the services and cloud components configured are as per the design specification and expected policies. Scope covers (but is not limited to) the following
  - Server configuration
  - Storage services
  - Network components
  - Security components
  - Logs configuration
  - Access components.
- Verify the results of vendor audits and assess the availability of procedural and technical controls. Following certification/ reports may be referred -



- Verify if the services and cloud components are operating as per the design specifications. Scope covers (but is not limited to) to the following
  - Verification of key management
  - Verification of security settings
  - Challenge testing to access controls
  - Challenge testing to firewall features
  - Verification of time synchronisation
  - Verification of response time and network connectivity.
- Verify if application migration (if applicable) is performed correctly. Scope covers (but is not limited to) to the following
  - Verification of data transfer
  - Verification of adequate access controls
  - Verification of critical functionalities (Regression testing based on risk)
- Raise defects (if any), perform retesting and track defects for closure
- Maintain traceability between requirements and test protocols.

Reporting phase

All the qualification activities performed for the implementation should be summarised and kept ready in a controlled manner as defined by the organisation's document management procedure. This includes consolidation of all documents including SLAs and SOPs to maintain the qualified state of the cloud setup.

Typical deliverables - Test results, Defect summary reports, Qualification summary reports, SOPs to maintain compliance

- Summarise the test results in test summary reports
- Summarise the defects raised during testing in the defect summary report
- Summarise qualification activities along with deviations from the initial qualification plan (if any)
- Define SOPs to maintain operational compliance of the infrastructure
  - User access management
  - Audit trail review
  - Records retention
  - Incident and problem management
  - Backup and restoration

  - Business continuity management
  - Performance monitoring
  - Incident management
  - Change control and configuration
  - Archiving and retrieval.
- Consolidate all the documents required to provide assurance during any regulatory inspection

Operational phase

When the cloud setup is up and running, adequate controls must be enabled for proper monitoring. Changes pushed by the cloud service provider need to be controlled and regular assessment of vendor audit reports are to be performed.

Typical deliverables- Reports of vendor's continuous monitoring, organisation's operational review reports, organisation's periodic review reports

- Perform operational maintenance activities as per the defined SOPs
- Review infrastructure and services under regulated organisation's control
  - Perform operational reviews for change requests, incidents, user access, audit trail and others at a defined periodicity based on GxP risk
  - Perform periodic review of complete data structure/ infrastructure components compliance state as per the organisational QMS and GxP criticality
- Reviews of infrastructure and services under vendor's control
  - Perform continuous monitoring on the automated alerts with daily reporting
  - Review vendor audit reports and certification on a quarterly/half yearly/yearly basis to assess the compliance state
  - Review and revise SLAs based on any changes made to the infrastructure components or change in business requirements.

Maintaining changes in a regulated environment

One of the key concerns for regulated organisations is controlling the regular changes and upgrades in the cloud services. It is expected to prospectively validate any features before being used in GxP environment; hence additional measures are needed.

Continuous regression testing

- Identify key functionalities and regulatory requirements (audit trail, system security, password protection etc.) to be met by the system
- Maintain a separate test environment for testing deployments
- Use automation techniques to validate the system continuously for intended use
- Review and maintain reports.

Monitoring upcoming changes

Service providers should inform the regulated organisations on the upcoming changes and should have the major upgrades listed down well in advance. SLAs should be set in place to restrict number of releases in a time frame and the availability and adequacy of the SLAs should be verified during validation testing.

Compliance in a DevOps model

DevOps implementation is gaining traction in IT organisations and can be utilised by life sciences organisations to stay compliant and support shorter validation cycles. Traditional validation practices with agile methodology required creating and deploying codes in small packages that are created on development environment, tested on quality environment, and deployed on production environment followed by the next sprint. DevOps approach ensures that compliance and security concerns are dealt in the early stages of development.

3. Compliance risks in cloud adoption

Life sciences organisations operating in GxP areas like research and development are still hesitant in embracing cloud technology. However, implementation of adequate controls and compliance checkpoints can mitigate data integrity and security risks and help stay compliant.

Parameter	Risk	Mitigation
Application/ data migration	Loss of data and lack of documented evidence when migrating traditional software, data, infrastructure and applications to cloud.	• Identify required security control • Leverage tools provided by cloud providers • Run pre and post migration qualification tests.
Data security	Lack of visibility about the exact location of data storage on cloud. Loss or leakage of data due to improper access management.	• Identify GxP critical data and decide to use private, hybrid or public cloud • Set adequate access controls for data and leverage leakage prevention tools • Encrypt all data in transit and rest with proper encryption key rotation policy.
Applicable data laws	Local laws, such as privacy laws and data localisation laws in Europe, may intervene when it comes to sharing of GxP critical or personal data outside the country	• Identify GxP and Non-GxP data that have data localisation restrictions • Leverage distributed geographic locations of cloud service providers • Assess the need of private cloud solutions.
Lack of resources and expertise	Lack of trained internal resources on new processes and platforms in the cloud infrastructure can be a major challenge	• Understand the shared responsibility model and define required skillset • Leverage third party providers for operations management • Automate routine processes • Build a culture of continuous learning in the firm.
Overreliance on vendors	The selection of vendors and performance of third-party cloud vendors heavily impact the performance of the resources and the credibility of the organisation	• Identify the requirements and assess need of multi-cloud deployment • Consider leveraging hybrid cloud deployment models.
Governance and responsibility	Due to the shared responsibility, maintaining governance standards and providing assurance on operational compliance can become a challenge	• Understand the shared responsibility model of the cloud service provider • Have proper SLAs and contracts in place to ensure governance commitment • Create a cloud governance framework • Ensure that an incident management plan is in place.
Continuous change	The cloud model is continuously evolving with regular updates and patch fixes pushed by the cloud service provider. Regulatory bodies expect companies to provide documented verification of these changes	• Define SLAs and contracts towards service commitments • Be up to date with the changes and perform periodic validations • Perform continuous monitoring and have a periodic review framework in place.

4. Way forward

As cloud-based IT Infrastructure is being gradually adopted across life sciences value chain, it is essential that opportunities and threats associated with cloud implementation are well mapped and defined. If the path to cloud adoption is not a well thought out strategy and technology partners are not aligned with the company's objective; it can lead to serious performance and compliance issues. However, when they are, it could open new avenues for implementing strategic and innovative solutions.

KPMG in India contacts:

Preeti Devi
Associate Partner
T: +919491257789
E: preetidevi@KPMG.com

Sameen Ahmed
Associate Director
T: +919540751999
E: sameenahmed@KPMG.com

home.kpmg/in

Follow us on:
home.kpmg/in/socialmedia