VIEWPOINT

COMPUTER SYSTEM VALIDATION IN CLOUD COMPUTING

Infosys®
Navigate your next

Computer System Validation – An Introduction

Computer System Validation in the pharmaceutical sector involves establishing documented evidence that a system, process or method consistently leads to results that meet pre-determined specifications. Validation is crucial for ensuring the safety, efficacy & quality of pharmaceutical products. Regulatory agencies such as FDA and EMA, require the systems to be validated to ensure patient safety, product quality and data integrity.

Understanding Cloud Systems

A cloud system, often referred to as Cloud computing, is a technology that allows users to access and store data, applications and services over the internet instead of relying on local servers.

Types of Cloud Services:

- **Infrastructure as a Service (IaaS):** This model provides virtualized computing resources over the internet. Users can rent servers, storage and networking capabilities on pay-as-you-go basis.
- **Platform as a Service (PaaS):** This service provides a platform allowing developers to build, deploy and manage applications without the complexity of managing the infrastructure.
- **Software as a Service (SaaS):** This model delivers software applications over the internet on a subscription basis. Users access the software via web browsers without needing to install or maintain it locally.

Deployment Models:

- **Public Cloud:** Services & infrastructure are provided off-site over the internet and shared across multiple organizations. Providers are responsible for the management, security and maintenance of the resources
- **Private Cloud:** Resources are dedicated to a single organization and can be hosted on-site or by a third-party provider. This model offers more control & customization.
- **Hybrid Cloud:** This combines public & private cloud, allowing data and applications to be shared between them for greater flexibility and scalability.

Difference between Cloud and On-premises systems

When managing applications and data in regulated industries, organizations often weigh the differences between "Cloud systems" and "On-premise systems". These choices directly impact scalability, compliance, and overall operations in GxP environments. Understanding their benefits, limitations, and use cases is crucial for ensuring regulatory compliance and operational efficiency.

Cloud System	On-premise System
Cloud systems use remote servers to store and process data, providing access via the internet.	On-premises systems rely on local servers and infrastructure, offering high levels of control.
Cloud systems allow organizations to scale their infrastructure as needed, avoiding substantial capital investment in hardware	On-prem systems come with high initial costs and can lack the flexibility of cloud-based options.
Cloud solutions are quicker to implement and deliver automatic updates, aligning systems with current regulatory requirements.	Keeping On-premises system up to date can be resource-intensive, especially when regulations or standards evolve quickly.
Cloud systems enable remote access, allowing teams in different regions to collaborate seamlessly	With data stored on-site, on-premise solutions provide confidence in compliance with GxP guidelines
Cloud system validation benefits from vendor-supplied documentation	Validation in an on-premise system requires detailed planning and execution by internal teams.

The choice between cloud and on-premise systems depends on organizational needs, compliance requirements, and available resources. Cloud solutions excel in scalability, cost savings, faster deployments and global collaboration, making them an increasingly attractive option for organizations navigating the rigorous demands of regulated industries.

Challenges in Cloud Validation

While cloud systems offer significant benefits for regulated industries, they also introduce challenges that need to be addressed to ensure robust cloud validation and compliance with GxP requirements. Below are key challenges associated with cloud validation:

Vendor Dependency

Validation in a cloud environment often relies on vendor-provided documentation and infrastructure details. However, many cloud vendors treat aspects of their underlying infrastructure (e.g. networking, failover mechanisms, physical security, data routing & validated state of the infrastructure) as proprietary. This lack of visibility makes it difficult to fully validate system behavior, performance & security.

Data Security and Integrity Risks

Cloud systems place data on shared platforms or remote infrastructure, which can expose sensitive GxP-controlled data to potential security breaches. There are risks of loss/ corruption of data, unauthorized access and lack of visibility into backend operations, affecting their ability to verify how data is stored, processed and protected.

Ensuring Compliance Across Updates

Cloud systems frequently release automated updates to enhance functionality, fix bugs, or improve security. While this is beneficial from an innovation and maintenance standpoint, it possesses compliance risk. Updates may alter system behavior, configurations or interfaces. In SaaS & PaaS, organizations have limited control over backend changes made by the provider. Unverified changes can lead to non-compliance.

Shared Responsibility Model

In cloud environments, compliance responsibilities are shared between the organization and the cloud vendor. However, this division is misunderstood or not clearly defined in practice, which leads to compliance gaps or data breaches.
While vendors may offer infrastructure compliance (e.g., SOC 2, ISO certifications), the organization is still responsible for validating its applications, ensuring data controls, and performing risk management.

Audit and Regulatory Inspections

Cloud environments add complexity to regulatory audits due to the involvement of third-party vendors. Auditors may require visibility into the cloud provider's systems, processes, and security measures—areas outside the direct control of organizations. Preparing for audits in a multi-tenant or hybrid cloud system can be time-intensive and cumbersome.

Cross-Border Compliance

Cloud vendors often store data in multiple global data centers, which can result in cross-border data transfers. This introduces legal, regulatory, & privacy risks-particularly when sensitive data is moved across jurisdictions with different data protection laws e.g. General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA).

How to Address Challenges in Cloud Validation

While cloud-based systems bring efficiency and scalability, addressing the challenges associated with Cloud validation is critical for ensuring regulatory compliance in GxP environments. Solutions require a proactive, structured approach to manage security, validation, and vendor relationships while maintaining data integrity and compliance.

Vendor Assessment

To mitigate reliance on third-party vendors, perform a thorough Vendor assessment process to ensure the provider adheres to GxP, 21 CFR Part 11, and other regulations. Evaluate the vendor's security certifications (e.g., ISO 27001), review the System & Organization control (SOC) reports on a periodic basis to ensure that provided cloud services remain in compliance with relevant security, privacy, and operational standards and conduct regular audits of their systems wherever possible.

Strengthen Data Security and Integrity

Address data privacy and security concerns by implementing robust Encryption, user authentication, and access control mechanisms. Leverage role-based access control (RBAC) to limit data access to authorized users. Ensure all data transfers are encrypted (e.g., using HTTPS or VPN). Review the SOC 2 Type 2 reports to assess how effectively vendor manages data security, integrity, confidentiality, and availability over time.

Adopt Continuous Validation Processes

To handle frequent software updates in the cloud, establish clear SLAs with vendor defining an advance notification of updates, access to validation documents & regression testing results. Set up alerts for critical updates, security patches, or changes in data processing components.

Implementing change management process & Continuous validation strategies, such as regression testing and performance verification, can ensure changes introduced by updates do not affect compliance or critical system functionality.

Clarify the Shared Responsibility Model

Clearly define roles and responsibilities between the organization and the cloud vendor. For instance, while the vendor may be responsible for infrastructure, physical security or software security, the organization is typically responsible for application-layer validation, user management, and compliance with internal policies. These responsibilities must be explicitly managed, documented, and validated.
Ensure proper review of SOC reports, SLAs, shared responsibility documents, and Data processing agreements from cloud providers.

Audit / Inspection Readiness and Documentation

Ensure the cloud system is audit/inspection-ready by maintaining proper documentation of validation protocols, user access logs, and system usage. Ensure the contracts or SLAs includes the right to Audit, right to request vendor audit reports or third-party assessments. Periodically review the SOC 2 reports from the vendor.

Ensure Cross-Border Data Compliance

Tackle jurisdictional compliance (e.g., GDPR) by contracting vendors with in-region data centers when needed and closely monitoring where data is stored and processed, review and enforce Data processing agreements. This ensures alignment with local regulations and privacy laws.

Improving Effectiveness & Efficiency with GenAI

Significant manual effort that is repetitive in nature is required to be expended to maintain compliance with regulatory requirements, information security, audit/inspection- readiness. Using the intervention of GenAI, agents can be developed to perform these repetitive activities, which will also keep learning through every execution. These agents can be invoked at defined frequencies according to the risk and situation.

Summary

Addressing challenges in Cloud validation requires a holistic approach, involving strong vendor assessment, continuous validation strategies, secure configuration, and proper governance. By establishing proactive controls around validation, collaboration, regulatory alignment and appropriate technological intervention, organizations can ensure that cloud systems meet GxP compliance while benefiting from the flexibility and efficiency that cloud technology offers.

Authors

Deepti Negi
Consultant LSDCG

Akarsh Srivastava
Sr. Consultant LSDCG

For more information, contact askus@infosys.com

Infosys®
Navigate your next