

# A Framework for Cloud Validation in Pharma

Pravin Ullagaddi<sup>1,2</sup>

<sup>1</sup>Plaster School of Business, University of the Cumberlands, Williamsburg, KY, USA

<sup>2</sup>Pacific Biolabs, Hercules, CA, USA

Email: pullagaddi05213@ucumberlands.edu

**How to cite this paper:** Ullagaddi, P. (2024)  
A Framework for Cloud Validation in Pharma.  
*Journal of Computer and Communications*,  
12, 103-118.  
<https://doi.org/10.4236/jcc.2024.129006>

**Received:** August 25, 2024

**Accepted:** September 17, 2024

**Published:** September 20, 2024

Copyright © 2024 by author(s) and  
Scientific Research Publishing Inc.  
This work is licensed under the Creative  
Commons Attribution International  
License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## Abstract

The pharmaceutical industry's increasing adoption of cloud-based technologies has introduced new challenges in computerized systems validation (CSV). This paper explores the evolving landscape of cloud validation in pharmaceutical manufacturing, focusing on ensuring data integrity and regulatory compliance in the digital era. We examine the unique characteristics of cloud-based systems and their implications for traditional validation approaches. A comprehensive review of current regulatory frameworks, including FDA and EMA guidelines, provides context for discussing cloud-specific validation challenges. The paper introduces a risk-based approach to cloud CSV, detailing methodologies for assessing and mitigating risks associated with cloud adoption in pharmaceutical environments. Key considerations for maintaining data integrity in cloud systems are analyzed, particularly when applying ALCOA+ principles in distributed computing environments. The article presents strategies for adapting traditional Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ) models to cloud-based systems, highlighting the importance of continuous validation in dynamic cloud environments. The paper also explores emerging trends, including integrating artificial intelligence and edge computing in pharmaceutical manufacturing and their implications for future validation strategies. This research contributes to the evolving body of knowledge on cloud validation in pharmaceuticals by proposing a framework that balances regulatory compliance with the agility offered by cloud technologies. The findings suggest that while cloud adoption presents unique challenges, a well-structured, risk-based approach to validation can ensure the integrity and compliance of cloud-based systems in pharmaceutical manufacturing.

## Keywords

Computerized Systems Validation, Risk-Based Approach, Data Integrity, Pharmaceutical Manufacturing, Cloud Validation

## 1. Introduction

The pharmaceutical industry has long adopted advanced technologies to enhance drug development, manufacturing processes, and quality control. In recent years, the integration of computerized systems has become ubiquitous, revolutionizing various aspects of pharmaceutical operations [1]. These systems range from laboratory information management systems (LIMS) to enterprise resource planning (ERP) software, playing crucial roles in data management, process control, and regulatory compliance. As the industry continues to evolve, there has been a significant shift towards cloud-based systems. This transition is driven by the numerous advantages cloud computing offers, including scalability, cost-effectiveness, and improved accessibility [2]. However, adopting cloud-based solutions in a highly regulated environment like pharmaceutical manufacturing presents unique challenges, particularly in computerized systems validation (CSV) and data integrity assurance.

The importance of validation in ensuring data integrity cannot be overstated. In the pharmaceutical context, data integrity is not merely a technical concern but an essential factor that directly impacts patient safety and product quality. Regulatory bodies worldwide, including the U.S. Food and Drug Administration (FDA) and the European Medicines Agency (EMA), have emphasized the need for robust data integrity practices in Good Manufacturing Practice (GMP) environments [3] [4]. As cloud-based systems become more prevalent, traditional approaches to CSV are being challenged. The dynamic nature of cloud environments, shared responsibility models, and the potential for rapid changes in infrastructure and software necessitates re-evaluating validation strategies [5]. This paper argues that a risk-based approach to validating cloud-based computerized systems is essential for enhancing data integrity in pharmaceutical manufacturing while navigating the complexities of modern IT infrastructures. By examining the evolving regulatory landscape, assessing the unique characteristics of cloud-based systems in pharmaceutical contexts, and exploring innovative validation methodologies, this research aims to provide a comprehensive framework for implementing effective Computerized Systems Validation (CSV) practices in cloud environments. The goal is to ensure that the benefits of cloud computing can be leveraged in pharmaceutical manufacturing without compromising the stringent requirements for data integrity and regulatory compliance.

## 2. Evolving Regulatory Landscape

The regulatory framework governing computerized systems in pharmaceutical manufacturing has evolved significantly in response to technological advancements and emerging data integrity challenges. Understanding this landscape is crucial for developing effective validation strategies for cloud-based systems [6].

### 2.1. Current GMP Requirements for Computerized Systems

Good Manufacturing Practice (GMP) regulations have long included provisions

for computerized systems. In the United States, 21 CFR Part 11 on Electronic Records and Electronic Signatures, introduced in 1997, laid the groundwork for using computerized systems in GMP-regulated environments [7]. This regulation outlines requirements for system validation, audit trails, and electronic signatures, among other aspects. Similarly, Annex 11 of the EU Good Manufacturing Guidelines (GMP) Guidelines addresses computerized systems in Europe, emphasizing the need for validation and quality assurance throughout the system lifecycle [8]. Various guidance documents and industry standards have supplemented these foundational regulations, such as the Good Automated Manufacturing Practices (GAMP 5), which provides a risk-based approach to computerized system compliance and validation [9].

## 2.2. FDA Guidance on Data Integrity and Compliance

Recognizing the vital role of data integrity in ensuring product quality and patient safety, the FDA has issued specific guidance on data integrity in GMP environments. The guidance “Data Integrity and Compliance with Drug CGMP” emphasizes the ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, Accurate, plus Complete, Consistent, Enduring, and Available) as fundamental to maintaining data integrity [3]. This guidance extends to all GMP records, including those generated and maintained by computerized systems. It addresses key concerns such as shared login accounts, audit trail reviews, and the appropriate use of computer system administrator privileges. The FDA’s stance on data integrity applies equally to paper-based and electronic systems, including those hosted in cloud environments.

## 2.3. EMA and Other International Regulatory Perspectives

The European Medicines Agency (EMA) has also recognized the importance of data integrity in evolving IT landscapes. In 2016, the EMA published “Data Integrity” guidance that aligns closely with FDA perspectives while providing additional context for European regulatory frameworks [4]. This document emphasizes risk management approaches and the need for a data governance system that spans the entire data lifecycle. Other regulatory bodies, such as the Pharmaceutical Inspection Co-operation Scheme (PIC/S), have contributed to the global conversation on data integrity and computerized systems validation. The PIC/S “Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments” provides harmonized guidance that is influential beyond its member countries [10].

## 2.4. GDPR and Data Protection

The General Data Protection Regulation (GDPR) has introduced significant considerations for cloud-based Computerized System Validation (CSV) in pharmaceuticals [11]. Key GDPR articles impact cloud validation processes: Article 25 (“Data Protection by Design and by Default”) requires integrating data protection

measures into system design; Article 32 (“Security of Processing”) necessitates appropriate security controls; and Article 35 mandates Data Protection Impact Assessments (DPIA) for high-risk processing [12]. These requirements extend traditional CSV practices to include specific privacy considerations. GDPR’s data residency requirements pose challenges for multi-region cloud deployments, necessitating strategies like data localization or regional cloud instances [13]. The Privacy by Design principle, central to GDPR, aligns with CSV but introduces new validation criteria, such as data minimization and the right to erasure [14] [15]. Consequently, cloud CSV in pharmaceuticals must now validate functionality, security, and privacy protection features, ensuring compliance with GMP regulations and GDPR standards [16].

### **3. Cloud-Based Systems in Pharmaceutical Manufacturing**

Integrating cloud-based systems in pharmaceutical manufacturing represents a significant paradigm shift in the industry’s information technology and data management approach. This transformation is driven by the need for greater efficiency, scalability, and global collaboration in an increasingly complex and competitive market. As the pharmaceutical sector navigates this digital transformation, it is essential to understand the nuances of cloud-based systems, their impact on manufacturing processes, and their validation and regulatory compliance challenges. At its core, cloud computing provides on-demand access to a shared pool of configurable computing resources [17]. In pharmaceutical manufacturing, these resources encompass various applications and services that support various aspects of the drug development and production lifecycle. The adoption of cloud-based systems in this highly regulated industry has been gradual but steady, with companies increasingly recognizing the potential benefits while grappling with the associated risks and compliance challenges.

One of the primary drivers for cloud adoption in pharmaceutical manufacturing is the need for more agile and responsive systems that can adapt to changing market demands and regulatory requirements. Traditional on-premises systems, while reliable, often lack the flexibility and scalability needed to support modern pharmaceutical operations. Cloud-based solutions promise rapid deployment, more accessible updates, and the ability to scale resources up or down based on demand [2]. Manufacturing Execution Systems (MES) have been at the forefront of this cloud migration. Cloud-based MES provides real-time monitoring and control of manufacturing processes, offering unprecedented visibility into production operations. These systems facilitate the collection and analysis of vast data, enabling manufacturers to optimize processes, reduce variability, and ensure consistent product quality. The cloud-based nature of these systems allows for seamless integration across multiple manufacturing sites, supporting global operations and standardization efforts [5]. Similarly, Laboratory Information Management Systems (LIMS) have evolved significantly with cloud adoption. Cloud-based LIMS

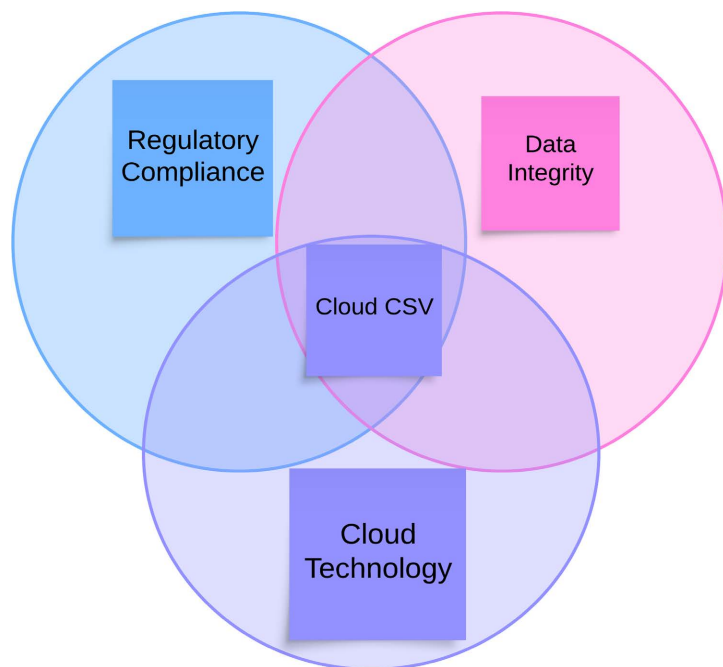
offers improved data management capabilities, enabling researchers and quality control teams to access and share data more efficiently. This enhanced accessibility has proven particularly valuable in supporting collaborative research efforts and facilitating remote work arrangements—a capability that became critical during the global COVID-19 pandemic. Moreover, cloud-based LIMS often come with advanced analytics tools to help identify trends and anomalies in laboratory data, potentially accelerating drug development timelines [18].

Quality Management Systems (QMS) have also benefited from the move to the cloud. Cloud-based QMS offers robust document control, change management, and quality event-tracking capabilities in an industry where regulatory compliance is paramount. These systems support consistent quality processes across global operations, ensuring all sites adhere to the same standards. Centralizing quality data in the cloud has improved visibility into quality metrics, enabling more proactive quality management approaches [19]. The adoption of cloud-based Clinical Trial Management Systems (CTMS) has revolutionized the conduct of clinical trials. These systems leverage cloud technology to streamline trial processes, from patient recruitment to data collection and analysis. The scalability of cloud-based CTMS is particularly beneficial given the variable and often unpredictable nature of clinical trial enrollment. Furthermore, these systems facilitate real-time data sharing among trial sites, sponsors, and regulatory authorities, potentially accelerating drug approval [20]. In supply chain management, cloud-based systems have emerged as critical tools for enhancing visibility and coordination across the complex networks that characterize pharmaceutical supply chains. These systems enable real-time tracking of raw materials, work-in-progress, and finished products, helping companies optimize inventory levels and respond more quickly to supply disruptions. The global accessibility of cloud-based supply chain systems has proven invaluable in managing the intricate logistics of pharmaceutical distribution, particularly in temperature-sensitive products like vaccines [21].

The benefits of cloud adoption in pharmaceutical manufacturing are significant; they come with unique challenges and risks that must be carefully managed. Data security and privacy concerns are paramount, given the sensitive nature of pharmaceutical data, which includes proprietary formulations, clinical trial results, and patient information. The storage of such data in cloud environments raises questions about unauthorized access and potential data breaches. To address these concerns, pharmaceutical companies must work closely with cloud service providers to implement robust security measures, including encryption, access controls, and regular security audits [6]. Compliance with pharmaceutical regulations in a cloud environment presents another layer of complexity. Regulatory bodies such as the FDA and EMA have established stringent requirements for data integrity, system validation, and traceability. Ensuring compliance with these regulations in a cloud environment, where a third-party provider manages the underlying infrastructure, requires re-evaluating traditional compliance

strategies. Pharmaceutical companies must establish clear delineations of responsibility with their cloud service providers and implement comprehensive audit trails that span both cloud and on-premises systems [5] [6] [14]. The dependency on internet connectivity inherent in cloud-based systems introduces a potential point of failure that must be carefully considered in manufacturing operations. While modern cloud architectures offer high levels of redundancy and reliability, pharmaceutical companies must implement robust contingency plans to ensure continuity of operations in the event of connectivity issues. This may involve maintaining local caches of critical data or implementing hybrid cloud solutions that combine cloud and on-premises resources [5].

The risk of vendor lock-in is another consideration when adopting cloud-based systems. As pharmaceutical companies integrate cloud solutions into their core processes, transitioning between providers can become increasingly challenging. This potential dependency on a single vendor must be weighed against the benefits of deep integration and customization. Companies should consider multi-cloud strategies to mitigate this risk and ensure their data and processes are as portable as possible [2]. Data residency issues present a unique challenge in the global pharmaceutical industry. Different countries and regions have varying requirements regarding the storage and processing of data within their borders. Cloud-based systems, which may distribute data across multiple geographic locations for redundancy and performance reasons, must be carefully configured to comply with these data residency requirements (Figure 1). This often necessitates close collaboration with cloud service providers to ensure that data storage and processing locations can be controlled and audited [22].



**Figure 1.** Cloud Validation at the intersection of Regulatory Compliance, Cloud technology, and Data Integrity.

## 4. Risk-Based Approach to Validation

The complexities introduced by cloud-based systems in pharmaceutical manufacturing necessitate re-evaluating traditional validation approaches. The dynamic nature of cloud environments, coupled with the critical importance of data integrity and regulatory compliance in the pharmaceutical industry, has led to the adoption of risk-based validation strategies. These strategies aim to ensure the reliability and compliance of cloud-based systems while leveraging their inherent flexibility and scalability. Risk-based validation is rooted in recognizing that not all aspects of a computerized system carry equal weight regarding their potential impact on product quality and patient safety. This approach aligns closely with regulatory guidance, notably the International Conference on Harmonisation (ICH) Q9 Quality Risk Management guidelines, emphasizing the importance of focusing quality management resources on areas of highest risk [23].

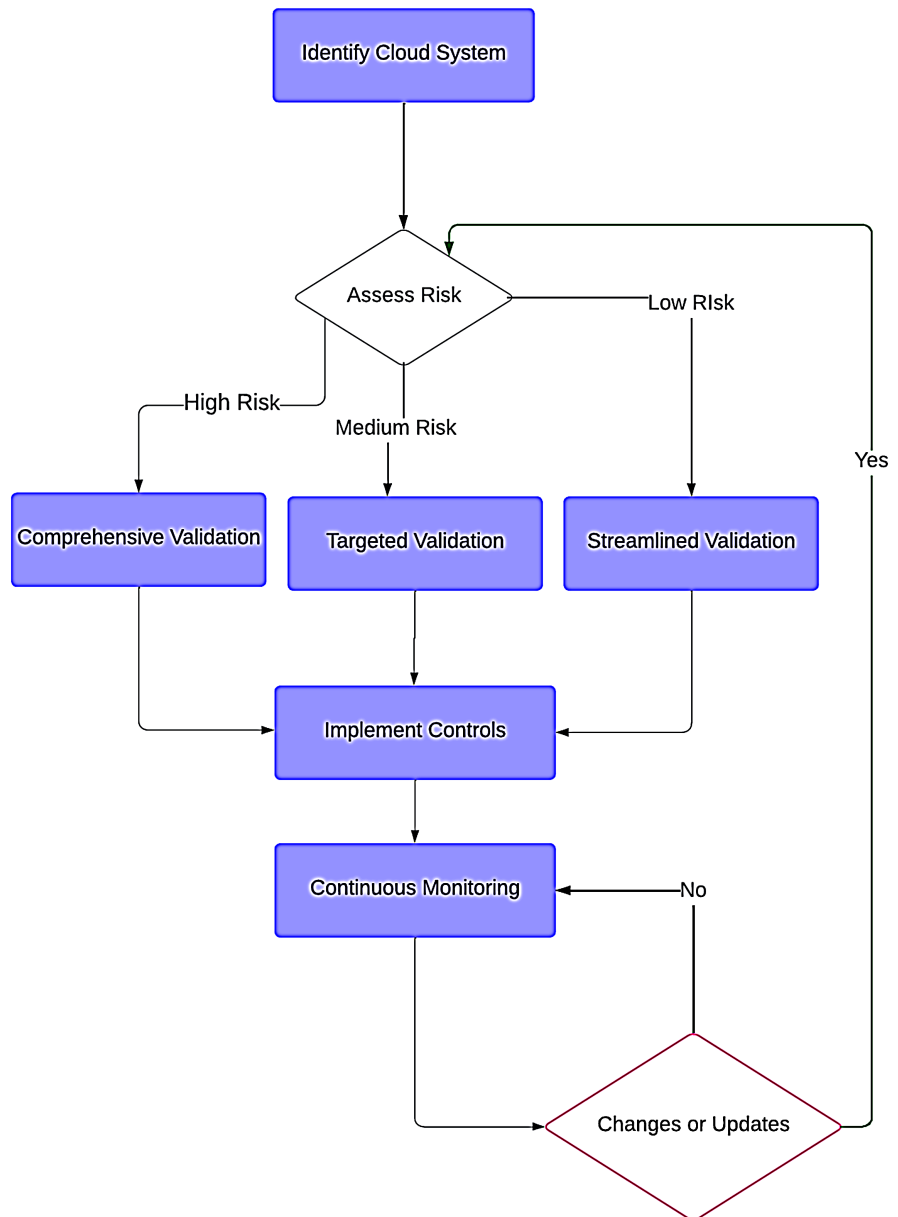
At its core, risk-based validation seeks to allocate validation efforts and resources in proportion to the level of risk associated with different aspects of a system. This approach requires a deep understanding of the system's functionalities, its role in manufacturing, and the potential consequences of system failures or data integrity breaches. By focusing validation efforts on the most critical aspects of a system, companies can achieve a more efficient and effective validation process without compromising on quality or compliance [24]. Applying risk-based validation principles becomes particularly relevant in the context of cloud-based systems. The shared responsibility model that characterizes most cloud computing arrangements introduces new variables into the validation equation. While cloud service providers typically assume responsibility for the security and reliability of the underlying infrastructure, pharmaceutical companies remain accountable for their processes and data compliance. This division of responsibilities necessitates a collaborative approach to validation, where the efforts of the pharmaceutical company and the cloud service provider are leveraged to ensure overall system compliance [25].

Implementing a risk-based approach to validating cloud-based systems begins with a comprehensive risk assessment. This assessment should consider various factors, including the criticality of the data handled by the system, the complexity of the system architecture and integrations, and the potential impact of system failures on product quality and patient safety. The risk assessment process should be iterative, with risks being re-evaluated throughout the system's lifecycle to account for changes in the system, the business processes it supports, or the regulatory landscape [5].

### Conceptual Framework for Risk-Based CSV

Risk-based computerized systems validation (CSV) in cloud environments integrates quality risk management principles with the distinctive characteristics of cloud computing. A graphical representation of the framework is shown in **Figure 2**. This comprehensive method utilizes the flexibility and scalability of cloud

technology to ensure adherence to regulatory compliance. Validation requires five interconnected steps.



**Figure 2.** Risk-based validation of cloud systems.

The initial stage, System Characterization, examines and records the cloud-based system. The first phase establishes the structure of the system, encompassing all elements and their interconnections and creating a visual representation of how data moves within the system and between external entities. The regulatory impact and significance of GMP processes are recognized. The concept of shared responsibility between pharmaceutical companies and cloud service providers is further explained in this step. The intended utilization of the system, as well as the responsibilities of the users and the controls on their access, are also elucidated to

clarify the system's extent and functioning.

Risk Assessment thoroughly evaluates potential dangers by analyzing the characteristics of the system. This phase involves identifying risks special to cloud computing, including concerns related to the location of data, the sharing of resources among several users, and the potential for service disruptions. An assessment is conducted to determine the probability and consequences of detected hazards on the integrity of data, quality of products, and safety of patients. Threats are evaluated based on predetermined acceptance criteria and ranked according to their severity and the criticality of the system. This step evaluates technical risks, such as data breaches and system failures, as well as compliance concerns, such as regulatory non-compliance, in order to determine the system's risk profile.

The Control Strategy Development phase involves designing and implementing risk reduction measures determined by a thorough risk assessment. Controls are implemented to ensure the integrity of cloud data, hence mitigating risks. This phase delineates the responsibilities for implementing and maintaining controls of the pharmaceutical business and cloud service provider. Controls must adhere to the ALCOA+ criteria, which include being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. The controls in this phase are adaptable and sensitive to the ever-changing nature of cloud settings. They incorporate measures to prevent and investigate risks, ensuring effective risk management.

The Validation Execution step verifies and records the extent to which the system conforms to the specified requirements. The conventional methods of IQ, OQ, and PQ are modified to suit the cloud environment at this stage. For IaaS and PaaS models, IQ places greater importance on configuration management and security controls than on physical installation. OQ prioritizes accurate design and customization to meet the specific requirements of pharmaceutical processes in SaaS models. PQ conducts comprehensive assessments of end-to-end procedures, data integrity, and performance across various operational scenarios. Whenever feasible, we employ automated testing to enhance efficiency and comprehensiveness. All validation activities and findings are compliantly documented to preserve a comprehensive record of the validation process.

The third phase, Continuous Monitoring, and Revalidation guarantees adherence and optimal functioning of the system in dynamic cloud environments. Continuous monitoring tools and processes identify deviations from the established state at this level. The revalidation requirements encompass significant alterations to the system and changes in regulations. Risks are continuously reevaluated to identify any new or modified hazards. Change management and impact assessments are used to handle system modifications. This process efficiently confirms system conformity following modifications through automated testing and validation methodologies. A continuous audit trail of system changes and validation activities records the system's state and compliance status.

The paradigm prioritizes the focus on maintaining data integrity throughout

these phases in order to uphold the ALCOA+ standards in distributed cloud environments. Continuous improvement feedback loops facilitate swift adaptation to technical advancements and emerging regulatory requirements. This risk-based method allows pharmaceutical organizations to prioritize validation efforts on essential system components, ensuring a balance between compliance needs and the flexibility of cloud technology. Pharmaceutical manufacturers can enhance compliance by tailoring validation efforts to the specific risks and characteristics of cloud-based systems, thereby maximizing the efficiency and effectiveness of cloud computing.

## 5. Data Integrity Considerations in Cloud Environments

Data integrity lies at the heart of pharmaceutical quality assurance and regulatory compliance. As the industry increasingly adopts cloud-based systems, ensuring data integrity in these distributed and dynamic environments has become a critical challenge [6]. Data integrity in the pharmaceutical context extends beyond mere accuracy; it encompasses the entire data lifecycle and is fundamental to patient safety and product quality. The U.S. Food and Drug Administration (FDA) and other regulatory bodies have emphasized the importance of ALCOA+ principles in maintaining data integrity. These principles stipulate that data should be Attributable, Legible, Contemporaneous, Original, and Accurate, with the “+” adding the requirements for data to be Complete, Consistent, Enduring, and Available [3]. While these principles were initially developed for paper-based systems, they apply equally to electronic data stored and processed in cloud environments.

In cloud-based systems, ensuring attributability presents unique challenges. The distributed nature of cloud computing, coupled with the potential for multiple users to access the system from various locations, requires robust user authentication and access control mechanisms. Implementing federated identity management systems that integrate with cloud services can help maintain clear audit trails of who accessed or modified data, when, and from where. Moreover, using electronic signatures that comply with 21 CFR Part 11 requirements becomes crucial in establishing the attributability of critical records in cloud environments [26].

Legibility in cloud systems extends beyond mere readability to include the proper formatting and presentation of data across various devices and platforms. Cloud-based systems must ensure that data remains legible and interpretable regardless of the device or application used to access it. This requirement necessitates careful consideration of data formats, metadata standards, and rendering technologies to maintain consistency across diverse access points [2]. The principle of contemporaneous data recording takes on new dimensions in cloud environments. The potential for real-time data capture and processing in cloud-based systems can enhance compliance with this principle. However, it also requires careful synchronization of timestamps across distributed systems and consideration

of time zone differences in global operations. Implementing precise time-stamping mechanisms and maintaining clear audit trails are essential in demonstrating data entry's contemporaneous nature [27]. Maintaining the originality of data in cloud systems involves technical and procedural controls. While cloud environments offer opportunities for easy data duplication and sharing, they also present risks of unauthorized alterations. Implementing robust version control systems and transparent policies on data modification and change management is crucial. Moreover, using blockchain or similar technologies to create tamper-evident audit trails is gaining traction to ensure data originality in cloud environments [28].

Accuracy in cloud-based systems relies heavily on the integrity of data transfer processes and the reliability of cloud infrastructure. Pharmaceutical companies must implement rigorous data validation processes at entry and during data migrations or transformations [6]. Regularly reconciling data across different parts of the cloud system and with any interfacing on-premises systems is essential to maintain data accuracy [18]. The "+" principles of ALCOA+ bring additional considerations in cloud environments. Ensuring data completeness requires careful design of data capture interfaces and implementation of checks to prevent incomplete records. Data consistency across distributed cloud systems necessitates sophisticated synchronization mechanisms and conflict resolution protocols. The enduring nature of data in the cloud must be guaranteed through robust backup and archival strategies, with transparent data retrieval processes extending beyond the operational life of specific cloud services [29].

Data availability in cloud systems presents both opportunities and challenges. While cloud platforms often offer high availability and redundancy, pharmaceutical companies must ensure that they maintain control over their data and can access it as needed for regulatory inspections or audits [30]. This requirement may necessitate hybrid cloud approaches or data replication strategies to maintain local copies of critical data [31]. Beyond these principles, ensuring data privacy and security in cloud environments is paramount, especially given the sensitive nature of pharmaceutical data. Encryption of data both in transit and at rest, rigorous access controls, and regular security audits are essential components of a comprehensive data integrity strategy for cloud-based systems. Furthermore, compliance with data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), adds another complexity to data management in global cloud environments [29].

## 6. Validation Strategies for Cloud-Based Systems

The validation of cloud-based systems in pharmaceutical manufacturing requires a paradigm shift from traditional validation approaches. The dynamic nature of cloud environments, coupled with the shared responsibility model between cloud service providers and pharmaceutical companies, necessitates innovative validation strategies to ensure compliance while leveraging the inherent benefits of cloud computing. Adapting the traditional Installation Qualification (IQ), Operational

Qualification (OQ), and Performance Qualification (PQ) model to cloud environments requires a nuanced approach. In Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) cloud models, the IQ phase may focus more on configuration management and verification of security controls rather than physical installation. For Software as a Service (SaaS) solutions, the emphasis shifts toward verifying the correct configuration and customization of the software to meet specific pharmaceutical process requirements [5].

The OQ phase in cloud validation must address the unique operational characteristics of cloud environments, including elastic scaling, multi-tenancy, and automated updates. Validation protocols must be designed to verify that the system performs as intended across various operational scenarios, including peak load conditions and during scaling events. Moreover, the OQ should thoroughly test data integrity controls, audit trail functionalities, and system interfaces, particularly those that bridge cloud and on-premises systems [25]. Performance Qualification in cloud environments extends beyond traditional performance metrics, including data consistency, latency, and availability assessments across geographically distributed access points. Given the critical nature of many pharmaceutical processes, PQ protocols should include rigorous testing of failover mechanisms, disaster recovery procedures, and business continuity capabilities inherent in the cloud solution [2].

The dynamic nature of cloud environments, with frequent updates and patches, challenges the traditional notion of a validated state. To address this, many organizations are adopting continuous validation approaches. This strategy involves implementing automated testing frameworks to verify system functionality and compliance following changes or updates rapidly. Continuous validation aligns well with agile development methodologies and DevOps practices increasingly adopted in the pharmaceutical IT landscape [26]. Leveraging automated testing and validation tools becomes crucial in cloud-based systems. These tools can help rapidly execute comprehensive test suites, verify data integrity, and generate the necessary documentation for regulatory compliance. Advanced technologies such as artificial intelligence and machine learning are beginning to play a role in predictive validation, identifying potential issues before they impact system performance or compliance [24] [25] [32].

Vendor assessment and management take on heightened importance in cloud-based CSV [27]. Pharmaceutical companies must conduct thorough due diligence on cloud service providers, assessing their quality management systems, security controls, and compliance with relevant regulations. Establishing clear Service Level Agreements (SLAs) that address performance, availability, data integrity, and compliance requirements is crucial. Moreover, pharmaceutical companies should maintain the right to audit their cloud service providers and access relevant compliance documentation [24] [33] [34]. The validation of cloud-based systems also necessitates a reevaluation of documentation strategies. While comprehensive documentation remains essential for regulatory compliance, the dynamic nature of

cloud environments requires more flexible and adaptable documentation approaches. Version-controlled, cloud-based documentation systems that can be rapidly updated to reflect system changes are becoming increasingly common. These systems must be designed to maintain the traceability and integrity of validation records over time [18] [35].

As the pharmaceutical industry leverages cloud technologies, validation strategies must evolve to address emerging challenges. The increasing use of multi-cloud and hybrid cloud architectures introduces new complexities in ensuring consistent validation across diverse environments. Furthermore, the adoption of edge computing in pharmaceutical manufacturing, particularly for real-time process control and data analytics, will require validation approaches that span the continuum from edge devices to cloud backends [35]. In conclusion, validating cloud-based systems in pharmaceutical manufacturing requires a holistic approach that addresses the unique characteristics of cloud environments while ensuring compliance with stringent regulatory requirements. By adopting risk-based, continuous validation strategies and leveraging advanced technologies, pharmaceutical companies can harness the benefits of cloud computing while maintaining the highest standards of data integrity and product quality.

Blockchain technology is used to improve and ensure data integrity in the pharmaceutical business. Blockchain, by its unchangeable and distributed record of transactions, has the potential to facilitate the secure and verifiable monitoring of validation along the whole lifecycle, guaranteeing adherence to regulatory standards. Regarding Quality Management Systems (QMS) for CSV, blockchain technology can be used to create an unchangeable record of information about quality, such as batch records, test results, and certificates of analysis [34] [35]. Combining blockchain with technologies like the Internet of Things (IoT) and artificial intelligence (AI) makes it possible to create intelligent and autonomous quality management systems. These systems can identify and address quality problems as they occur instantly. As blockchain technology advances and becomes more widely used in the pharmaceutical business, it is anticipated to substantially enhance data integrity, traceability, and adherence to regulations [36].

## 7. Conclusions

The adoption of cloud-based systems in pharmaceutical manufacturing represents a significant shift in how the industry approaches information technology and data management. While offering numerous scalability, flexibility, and global collaboration benefits, cloud technologies also introduce unique challenges in ensuring regulatory compliance and data integrity. We have examined the evolving regulatory context, the specific characteristics of cloud systems in pharmaceutical manufacturing, and the critical considerations for maintaining data integrity in cloud environments. The discussion of risk-based validation approaches and strategies for validating cloud-based systems highlights the need for a paradigm shift in validation methodologies to address the dynamic nature of cloud computing. As

we look to the future, the intersection of cloud computing, artificial intelligence, edge computing, and other emerging technologies will continue to reshape the pharmaceutical manufacturing landscape. These advancements promise to enhance drug development, production efficiency, quality, and innovation. However, they also present new challenges in ensuring regulatory compliance and maintaining the highest patient safety and product quality standards.

The key to successfully navigating this evolving landscape lies in adopting flexible, risk-based approaches to validation that can adapt to technological changes while maintaining rigorous data integrity standards and regulatory compliance. Pharmaceutical companies, technology providers, and regulatory bodies must collaborate to develop frameworks and best practices to keep pace with technological advancements. The goal of computerized systems validation in cloud environments remains unchanged: to ensure the reliability, integrity, and compliance of systems critical to pharmaceutical manufacturing. By embracing innovative validation strategies and leveraging cloud technologies, the pharma industry can enhance its ability to deliver safe, effective, and high-quality medications to patients worldwide.

### Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

### References

- [1] Haleem, A., Javaid, M. and Khan, I.H. (2019) Current Status and Applications of Artificial Intelligence (AI) in Medical Field: An Overview. *Current Medicine Research and Practice*, **9**, 231-237. <https://doi.org/10.1016/j.cmrp.2019.11.005>
- [2] Aceto, G., Persico, V. and Pescapé, A. (2020) Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *Journal of Industrial Information Integration*, **18**, Article ID: 100129. <https://doi.org/10.1016/j.jii.2020.100129>
- [3] Food and Drug Administration (2022) Data Integrity and Compliance with Drug CGMP: Questions and Answers. U.S. Food and Drug Administration.
- [4] European Medicines Agency (2016) Good Manufacturing Practice. European Medicines Agency. <https://www.ema.europa.eu/en/human-regulatory-overview/research-development/compliance-research-development/good-manufacturing-practice>
- [5] Miller, M. and Zaccheddu, N. (2021) Light for a Potentially Cloudy Situation: Approach to Validating Cloud Computing Tools. *Biomedical Instrumentation & Technology*, **55**, 63-68. <https://doi.org/10.2345/0899-8205-55.2.63>
- [6] Ullagaddi, P. (2024). Digital Transformation in the Pharmaceutical Industry: Enhancing Quality Management Systems and Regulatory Compliance. *International Journal of Health Sciences*, **12**, 31-43. <https://doi.org/10.15640/ijhs.v12n1a4>
- [7] Food and Drug Administration (1997) PART 11-Electronic Records; Electronic Signatures. Code of Federal Regulations.
- [8] European Commission (2011) EudraLex the Rules Governing Medicinal Products in the European Union Volume 4 Good Manufacturing Practice Medicinal Products for

- Human and Veterinary Use.  
[https://health.ec.europa.eu/system/files/2016-11/annex11\\_01-2011\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf)
- [9] International Society of Pharmaceutical Engineers (2008) GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems. International Society of Pharmaceutical Engineers.
- [10] Pharmaceutical Inspection Co-Operation Scheme (PIC/S) (2021) Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments.  
<https://www.gmp-compliance.org/files/guidemgr/PI%20041-1.pdf>
- [11] Cambroneró, M.E., Martínez, M.A., Llana, L., Rodríguez, R.J. and Russo, A. (2024) Towards a GDPR-Compliant Cloud Architecture with Data Privacy Controlled through Sticky Policies. *PeerJ Computer Science*, **10**, e1898.  
<https://doi.org/10.7717/peerj-cs.1898>
- [12] The European Parliament and the Council of the European Union (2016) General Data Protection Regulation.  
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- [13] Millard, C.J. (2021) Cloud Computing Law. Oxford University Press.
- [14] Ullagaddi, P. (2024) GDPR: Reshaping the Landscape of Digital Transformation and Business Strategy. *International Journal of Business Marketing and Management*, **9**, 29-35.
- [15] Cavoukian, A. (2009) Privacy by Design the 7 Foundational Principles Implementation and Mapping of Fair Information Practices.
- [16] Lalova-Spinks, T., De Sutter, E., Valcke, P., Kindt, E., Lejeune, S., Negrouk, A., *et al.* (2022) Challenges Related to Data Protection in Clinical Research before and during the COVID-19 Pandemic: An Exploratory Study. *Frontiers in Medicine*, **9**, Article ID: 995689. <https://doi.org/10.3389/fmed.2022.995689>
- [17] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology, Special Publication 800-145.  
[https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf?lspt\\_context=gdpr](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf?lspt_context=gdpr)
- [18] Paul, S., Gade, A. and Mallipeddi, S. (2017) The State of Cloud-Based Biospecimen and Biobank Data Management Tools. *Biopreservation and Biobanking*, **15**, 169-172.  
<https://doi.org/10.1089/bio.2017.0019>
- [19] Saleem Al-Shura, M., Zabadi, M.A., Abughazaleh, M. and Alhadi, M. (2018) Critical Success Factors for Adopting Cloud Computing in the Pharmaceutical Manufacturing Companies. *Advances in Economics and Business*, **6**, 168-178.  
<https://doi.org/10.13189/aeb.2018.060303>
- [20] Cresswell, K., Domínguez Hernández, A., Williams, R. and Sheikh, A. (2022) Key Challenges and Opportunities for Cloud Technology in Health Care: Semistructured Interview Study. *JMIR Human Factors*, **9**, e31246. <https://doi.org/10.2196/31246>
- [21] Abdallah, S. and Nizamuddin, N. (2023) Blockchain-Based Solution for Pharma Supply Chain Industry. *Computers & Industrial Engineering*, **177**, Article ID: 108997.  
<https://doi.org/10.1016/j.cie.2023.108997>
- [22] Studnia, I., Alata, E., Nicomette, V., Kaâniche, M. and Laarouchi, Y. (2018) A Language-Based Intrusion Detection Approach for Automotive Embedded Networks. *International Journal of Embedded Systems*, **10**, 1-12.  
<https://doi.org/10.1504/ijes.2018.089430>
- [23] International Conference on Harmonization (2015) ICH Guideline Q9 on Quality

- Risk Management Step 5.  
[https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use-ich-guideline-q9-quality-risk-management-step-5-first-version\\_en.pdf](https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use-ich-guideline-q9-quality-risk-management-step-5-first-version_en.pdf)
- [24] Choudharya, A.N. (2021) A Review on Pharmaceutical Validation and ITS Implications. *Journal of Medical Pharmaceutical and Allied Sciences*, **10**, 3951-3961.  
<https://doi.org/10.22270/jmpas.v10i6.1927>
- [25] O'Donnell, K., Greene, A., Zwitkovits, M. and Calnan, N. (2012) Quality Risk Management: Putting GMP Controls First. *PDA Journal of Pharmaceutical Science and Technology*, **66**, 243-261. <https://doi.org/10.5731/pdajpst.2012.00859>
- [26] Tian, F. (2017) A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things. 2017 *International Conference on Service Systems and Service Management*, Dalian, 16-18 June 2017, 1-6.  
<https://doi.org/10.1109/icsssm.2017.7996119>
- [27] Mehrtak, M., Seyed Alinaghi, S., Mohsseni Pour, M., Noori, T., Karimi, A., Shamsabadi, A., *et al.* (2021) Security Challenges and Solutions Using Healthcare Cloud Computing. *Journal of Medicine and Life*, **14**, 448-461.  
<https://doi.org/10.25122/jml-2021-0100>
- [28] Jahankhani, H., Kendzierskyj, S., Associate, J., Epiphaniou, G. and Al-Khateeb, H. (2019) *Blockchain and Clinical Trial: Securing Patient Data*. Springer.
- [29] Fiore, M., Capodici, A., Rucci, P., Bianconi, A., Longo, G., Ricci, M., *et al.* (2023) Blockchain for the Healthcare Supply Chain: A Systematic Literature Review. *Applied Sciences*, **13**, Article No. 686. <https://doi.org/10.3390/app13020686>
- [30] Ullagaddi, P. (2024) Leveraging Digital Transformation for Enhanced Risk Mitigation and Compliance in Pharma Manufacturing. *Journal of Advances in Medical and Pharmaceutical Sciences*, **26**, 75-86.  
<https://doi.org/10.9734/jamps/2024/v26i6697>
- [31] Sun, Y., Zhang, J., Xiong, Y. and Zhu, G. (2014) Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, **10**, Article ID: 190903. <https://doi.org/10.1155/2014/190903>
- [32] Rahman, M.A., Shakur, M.S., Ahamed, M.S., Hasan, S., Rashid, A.A., Islam, M.A., *et al.* (2022) A Cloud-Based Cyber-Physical System with Industry 4.0: Remote and Digitized Additive Manufacturing. *Automation*, **3**, 400-425.  
<https://doi.org/10.3390/automation3030021>
- [33] Ullagaddi, P. (2024) Digital Transformation in the Pharmaceutical Industry: Ensuring Data Integrity and Regulatory Compliance. *The International Journal of Business & Management*, **12**, 110-120.  
<https://doi.org/10.24940/theijbm/2024/v12/i3/bm2403-013>
- [34] Ullagaddi, P. (2024) Digital Transformation Strategies to Strengthen Quality and Data Integrity in Pharma. *International Journal of Business and Management*, **19**, 16-26. <https://doi.org/10.5539/ijbm.v19n5p16>
- [35] Ullagaddi, P. (2024) Safeguarding Data Integrity in Pharmaceutical Manufacturing. *Journal of Advances in Medical and Pharmaceutical Sciences*, **26**, 64-75.  
<https://doi.org/10.9734/jamps/2024/v26i8708>
- [36] Ullagaddi, P. (2024) Cloud Validation in Pharma: Compliance and Strategic Value. *International Journal of Business Marketing and Management*, **9**, 11-17.  
<https://ijbmm.com/paper/Sep2024/8340436651.pdf>