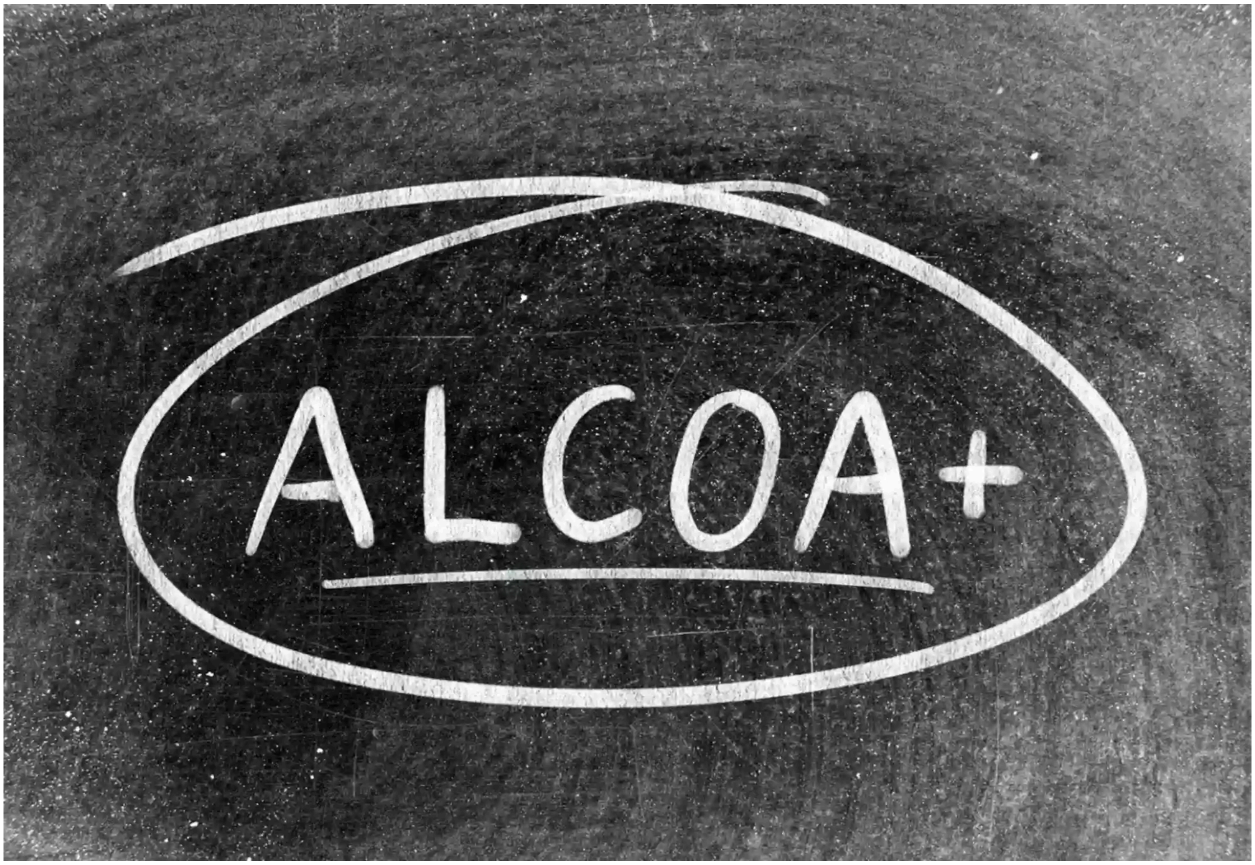
Data Integrity - A Cornerstone of Computer System Validation in Life Sciences



Why do we need Data Integrity?

Ensuring the safety and integrity of data is the primary objective for any computer system deployed in the Life Sciences industry, especially in regulated space. Data integrity signifies that data remains uncompromised and accurate throughout its lifecycle within the system, safeguarding its reliability and trustworthiness.

Guide to Data Integrity

- Many regulatory agencies worldwide have issued comprehensive guidance documents outlining expectations for data integrity in regulated industries, with the ALCOA principle serving as a fundamental aspect among them.
- ALCOA stands for Attributable, Legible, Contemporaneous, Original and Accurate.
    - Attributable – Data should have information about who performed the action and when it was performed.

  - Legible – Data should be readable and understandable to users.
  - Contemporaneous – Data should be recorded then and there when the action was performed.
  - Original – The original form of the data should be available.
  - Accurate – Data should be free from errors.
- Various iterations and enhancements of the ALCOA principle, such as ALOCOA+, have emerged, incorporating additional criteria like completeness, consistency, endurance, etc. for upholding data integrity standards.

Data Integrity in Computer System Validation

- A pivotal focus of Computer System Validation is to verify data integrity is achieved throughout the data life cycle in the computer system.
- In Risk-Based Validation, the risk level associated with each functionality within the system is assessed based on the potential impact on data integrity in the event of the functionality failure.
- To ensure data integrity, computer systems have technical controls (Access restrictions, electronic signature, audit trail, etc.) and procedural controls (data review and approval process) in place.
- Some systems have data validation/checks to add another layer of security to avoid incorrect data entered into the system.
- Many organizations integrate data integrity policies in the Quality Management System to keep a periodic check on data integrity.
- In environments where data concerning patient safety is managed, robust protocols for data archival, backup, and recovery are systematically implemented. The retention period for archived data is typically contingent upon organizational policies, ensuring adherence to regulatory standards and safeguarding critical patient information over time.
- In addition to all the above measures, training and awareness for the users handling sensitive data is very important to maintain data integrity. Many Robust Training Management Systems are now available in the market to ensure hassle-free training management.

Conclusion

Implementing data integrity measures may initially seem like a tedious task, but integrating these policies into the existing quality policies can significantly streamline the process. By aligning with the established guidelines, organizations can efficiently maintain data integrity and ensure compliance.

References

1. Data Integrity and Compliance With CGMP Guidance for Industry (fda.gov)
2. General Principles of Software Validation | FDA