GAMP GROUP

www.gampservices.com
sanjeev@gampservices.com

What Is Data Integrity?

Data integrity means that all data must be accurate, complete, and maintained in its original or true copy form throughout its lifecycle. Accurate and reliable data ensures that drugs are produced consistently and meet quality standards, essential for patient safety. It encompasses the principles of being attributable, legible, contemporaneous, original, and accurate (ALCOA).

Metadata plays a significant role in this context, serving as structured information that describes and makes data easier to retrieve, use, or manage. Without metadata, a data value remains meaningless, lacking the necessary context.

Ensuring data integrity means that any recorded information can be trusted to be true and unchanged, providing a reliable basis for decision-making in manufacturing and controlling pharmaceutical products.

Any compromise in data integrity can lead to serious consequences, including releasing substandard or harmful products, regulatory actions, and loss of public trust.

Key Concepts in Data Integrity

The key concepts in data integrity include:

ALCOA+ Principles

The ALCOA+ principles form the foundation of data integrity, ensuring data is reliable and accurate throughout its lifecycle. The principles are:

- **Attributable:** Clearly linked to the individual who created it.
- **Legible:** Easily readable and permanent.
- **Contemporaneous:** Recorded at the time of the activity.
- **Original:** The first record or a certified copy.
- **Accurate:** Free from errors.

Additionally, the data should be:

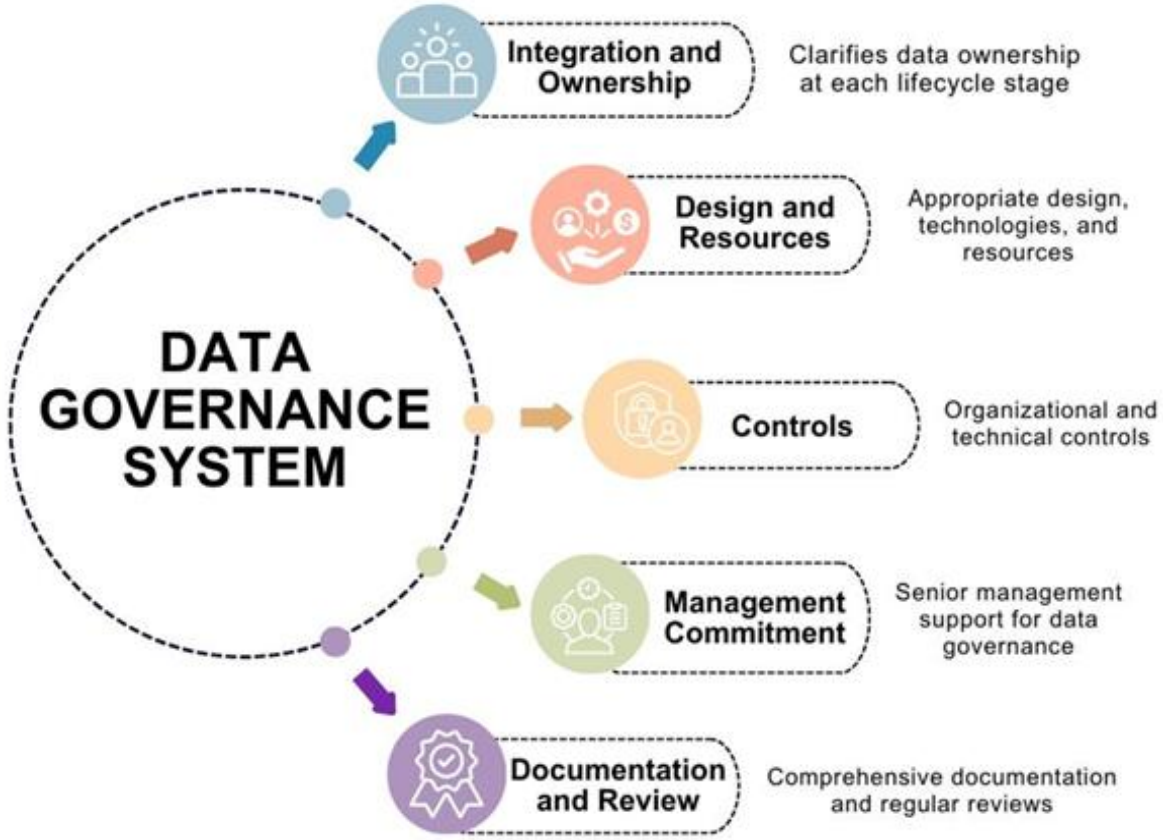
- **Complete:** Containing all necessary information.
- **Consistent:** Following a consistent format.
- **Enduring:** Available for the required duration.
- **Available:** Accessible for review and audit.

www.gampservices.com
sanjeev@gampservices.com

What Is Data Governance?

Data governance is a comprehensive system designed to ensure data integrity throughout its entire lifecycle. This means making sure that data is always accurate, reliable, and accessible, no matter how it's created, processed, stored, or used.

Implementing a data governance system isn't legally required, but it helps organizations manage data integrity risks effectively. Without it, data integrity efforts might be fragmented, leading to possible gaps in control.



Data Lifecycle

The data lifecycle refers to all the stages that data goes through, from its creation to its eventual disposal. This includes generating, processing, reporting, verifying, using, storing, and discarding data.

Throughout this lifecycle, data may move between different systems (e.g., from paper to digital) and different departments or organizations,

both internally (like production, quality control, and quality assurance) and externally (such as service providers).

Components of Data Governance Systems

The data governance systems include the following components:

Integration and Ownership

A good data governance system should be part of the overall Pharmaceutical Quality System. It should clarify who owns the data at each stage of its lifecycle and ensure processes and systems are designed to maintain data integrity, including preventing unauthorized changes or deletions.

Design and Resources

For a data governance system to be effective, it needs to be well-designed and use appropriate technologies and security measures. This requires expertise in data management and integrity. Organizations must allocate sufficient resources to design, develop, operate, and monitor these systems, taking into account the complexity of their operations and the importance of the data.

Controls

Controls are essential to maintaining data integrity and should be proportional to the risk involved. These controls can be:

- **Organizational:** Establishing clear procedures for handling data, training staff, regularly verifying data, conducting self-inspections, and involving experts in data management.
- **Technical:** Validating computerized systems, using automation to reduce human error, and employing technologies that enhance data security and management.

Management Commitment

Senior management must be committed to data governance, understanding its importance, and fostering a culture that supports data integrity. Employees should feel empowered to report any issues or suggest improvements without fear of reprisal, which helps prevent data falsification or deletion.

Documentation and Review

All data governance practices should be documented and regularly reviewed as part of the Pharmaceutical Quality System. This ensures that they remain effective and up-to-date.

Data Criticality

The significance of data varies depending on the decision it influences and its impact on product quality or safety. For example, data used to make batch release decisions is more critical than warehouse cleaning records. Similarly, assay data for an active pharmaceutical ingredient (API) has a greater impact on product quality and safety than tablet friability data.

Data Risk

All GMP/GDP data must meet data integrity requirements, but assessing data criticality helps prioritize efforts. The rationale for this prioritization should be documented according to quality risk management principles.

Data risk assessments should evaluate the likelihood of data being altered, deleted, lost, or falsified, and how easily such actions can be detected. Measures should be in place to prevent unauthorized activity and increase the visibility of changes.

Factors Increasing Data Risk

Complex processes, inconsistent methods, and subjective outcomes increase the risk of data failure. In contrast, simple, well-defined processes with objective tasks reduce risk. Risk assessments should focus on business processes, evaluating data flows, and methods of data generation and processing, rather than just IT system functionality.

Data Governance System Review

The effectiveness of data integrity control measures should be periodically assessed through self-inspections (internal audits) or other review processes to ensure that controls over the data lifecycle are functioning as intended.

In addition to routine data verification checks, self-inspections should include:

- Verifying continued understanding of good data management practices among personnel.
- Reviewing the consistency of reported data against raw entries.
- Sampling computerized system logs or audit trails to ensure accurate reporting of relevant information.
- Analysing quality system metrics that may indicate the effectiveness of data governance.

An effective review of the data governance system demonstrates an understanding of how company behaviours interact with organizational and technical controls. The results of the review should be communicated to senior management and used to assess any residual data integrity risks.

Comparison Between Data Integrity and Data Governance

ASPECT	DATA INTEGRITY	DATA GOVERNANCE
DEFINITION	Accuracy, consistency, and reliability of data	Framework for managing data policies and practices
SCOPE	Ensuring data remains accurate and unaltered	Includes data integrity and broader management
FOCUS	Maintains data quality and prevents changes	Manages overall data handling, integrity, security, and compliance
KEY PRINCIPLES	ALCOA+	Policies, standards, stewardship, quality management, compliance, security, architecture, lifecycle management
IMPLEMENTATION	Controls, checks, and validation processes	Comprehensive framework with policies and systems
MAIN ACTIVITIES	Regular audits, validations, access controls	Policy enforcement, role assignments, quality and security management
OUTCOME	Reliable and accurate data for decision-making	Effective, compliant, and secure data management

As a GAMP Group,We have Team of SMEs for Comprehensive Data Integrity GAP assessment, DIRA, Data Integrity Audit, Data Governance Program Development & Implementation, Data Integrity Consultation & Remediation Projects.