Stay Compliant and Connected with the Latest Technology

Expert Insights

SARTORIUS

Wiley Analytical Science

Contents

Editorial

Dear Readers,

The lab of the future is digital. Correct data is fundamental in a quality control environment. Inaccuracies can lead to wrong decisions, compromising product safety and quality. It can have a negative impact on product costs and more importantly on patient health and safety. Today's laboratories are changing rapidly to prevent this problem by becoming "smarter", by automating technologies and using digital science solutions.

Some of the main challenges in this process of change include:

- Maintaining data integrity
- IT integration
- Creating efficient workflows

This eBook presents an overview of compliance and connectivity solutions and shows how the simple weighing process in the lab can be improved through new technologies that are leading to higher sample throughputs, workflow efficiency, and reproducibility of data and results.

The content of this eBook consists of:

- A summary of Wiley's book "Laboratory Control System Operations in a GMP Environment", discussing a practical approach to the implementation of connectivity and compliance.
- Summaries of articles on data integrity within the biopharmaceutical sector, data integrity of healthcare information, and digitalization in laboratories of the pharmaceutical industry.
- Case studies
- Interview with a product specialist

Enjoy the read!

Róisín Murtagh,
Editor at Wiley Analytical Science

BACK TO CONTENTS

Laboratory control system operations in a GMP environment

Adapted from David M. Bliesner

Book

In recent years, the US Food and Drugs Administration (FDA) has observed violations of the current good manufacturing practice (cGMP) regulations concerning data integrity.

The FDA defines data integrity as complete, consistent, and accurate data, which should be attributable, legible, contemporaneously recorded, original or genuine copy, and accurate (ALCOA). In addition, other organizations have included a "+" to the acronym which adds "complete, consistent, enduring, and available".

On the other hand, data governance is defined as the sum of arrangements, which assure data integrity. These arrangements will ensure a complete, consistent, and accurate record throughout the data lifecycle. Data governance should be integral to the pharmaceutical quality system, should address ownership, and consider the design, operation, and monitoring of processes/systems to comply with the principles of data integrity, including control over intentional and unintentional changes to, and deletion of information.

Data governance and data integrity have become a cottage industry within the regulatory compliance and cGMP consulting community. This level of increased scrutiny and required actions is a positive development for the industry but has a large source of information to attempt, understand, and apply. This chapter aims to address the specifics of data governance and data integrity within the laboratory control system (LCS).

Description of the laboratory data governance and data integrity

The purpose of the data governance system is to implement policies and procedures, which allow the full reconstruction of good manufacturing practice (GMP) activities by retrieving complete information relating to the production, testing, and release of a manufactured batch of drug or drug product.

The data governance and data integrity of the laboratory should include at least nine individual components.

I. Policy for data governance will be unique to each organization and should contain the following elements:
   - Explanation of the purpose of the data governance system
   - Graphical description of the data lifecycle (see Fig. 1)
   - Description of roles and responsibilities
   - Link the data governance system to the LCS and its sub-elements
   - Lists the related standard operating procedures (SOPs)
   - Lists of data governance and data integrity
   - Descriptions of components shown in the data governance and data integrity hierarchy (see Fig. 2):
     - Procedural controls
     - Technical controls
     - Data maps and data walks
     - Risk identification, ranking, and filtering
     - Data review
     - Data and operational audits
     - Employee awareness and training
     - Management oversight
   - Regulatory and industry data integrity references

II. List operational procedures, which are SOPs, and provide guidance on subjects that impact directly or indirectly on how data are generated, processed, reviewed, reported, stored, retrieved, achieved, and destroyed.

   Examples of typical SOP titles associated with laboratory operations that impact data integrity are:

   - Laboratory document control system
   - Laboratory good documentation practices
   - Installation, operational, and performance qualification (IQ/OQ/PQ) of laboratory equipment
   - Laboratory equipment lifecycle management

BACK TO CONTENTS

Figure 1

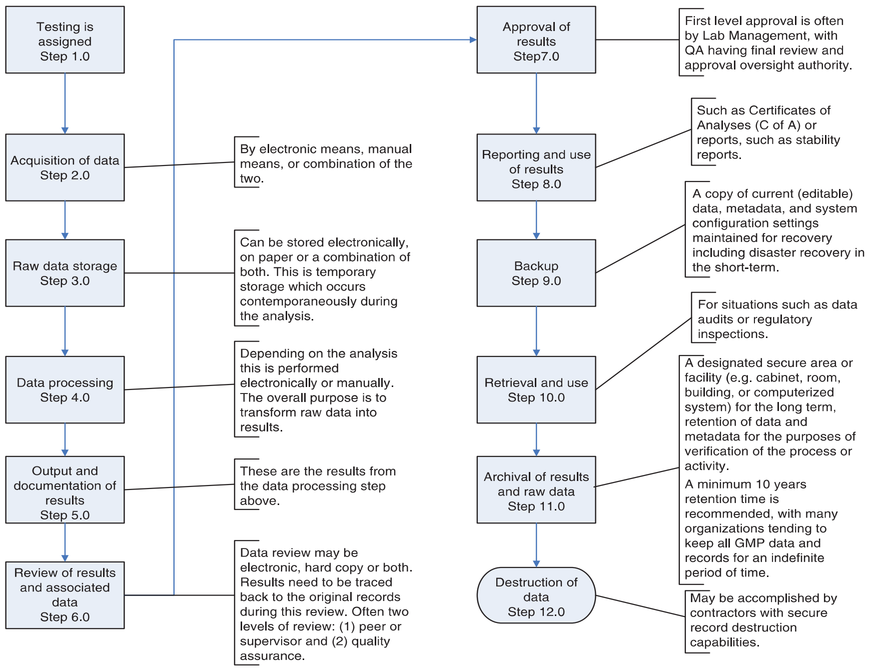

Testing is assigned Step 1.0
Acquisition of data Step 2.0
By electronic means, manual means, or combination of the two.
Raw data storage Step 3.0
Can be stored electronically, on paper or a combination of both. This is temporary storage which occurs contemporaneously during the analysis.
Data processing Step 4.0
Depending on the analysis this is performed electronically or manually. The overall purpose is to transform raw data into results.
Output and documentation of results Step 5.0
These are the results from the data processing step above.
Review of results and associated data Step 6.0
Data review may be electronic, hard copy or both. Results need to be traced back to the original records during this review. Often two levels of review: (1) peer or supervisor and (2) quality assurance.
Approval of results Step7.0
First level approval is often by Lab Management, with QA having final review and approval oversight authority.
Reporting and use of results Step 8.0
Such as Certificates of Analyses (C of A) or reports, such as stability reports.
Backup Step 9.0
A copy of current (editable) data, metadata, and system configuration settings maintained for recovery including disaster recovery in the short-term.
Retrieval and use Step 10.0
For situations such as data audits or regulatory inspections.
Archival of results and raw data Step 11.0
A designated secure area or facility (e.g. cabinet, room, building, or computerized system) for the long term, retention of data and metadata for the purposes of verification of the process or activity.
A minimum 10 years retention time is recommended, with many organizations tending to keep all GMP data and records for an indefinite period of time.
Destruction of data Step 12.0
May be accomplished by contractors with secure record destruction capabilities.

Fig. 1: *The lifecycle of laboratory data.*

Figure 2

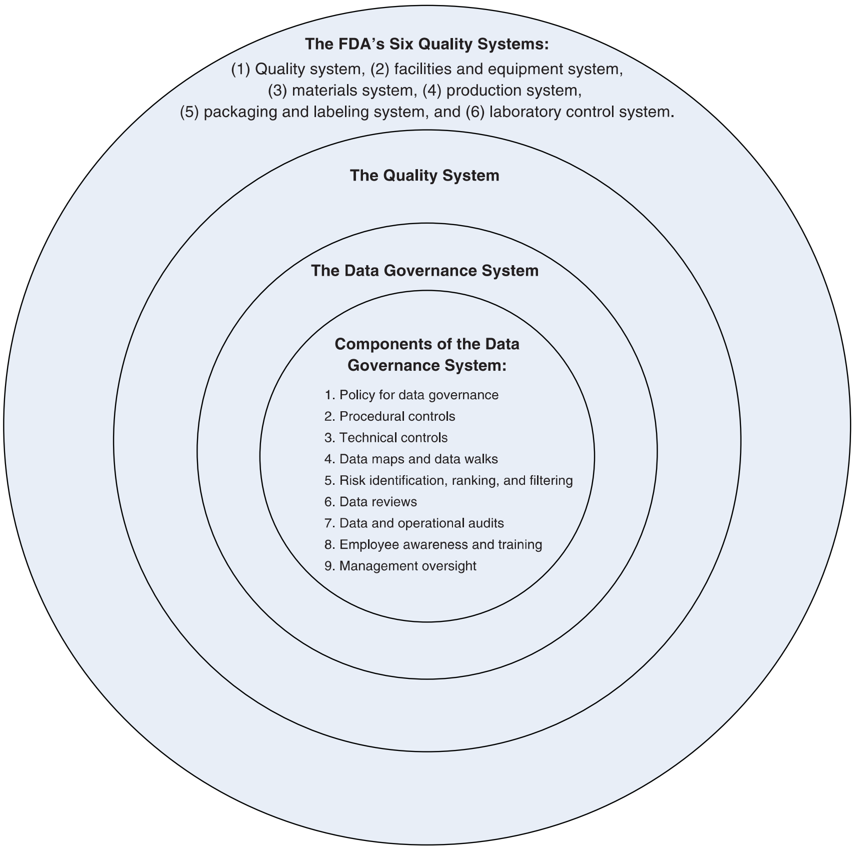

The FDA's Six Quality Systems:
(1) Quality system, (2) facilities and equipment system,
(3) materials system, (4) production system,
(5) packaging and labeling system, and (6) laboratory control system.
The Quality System
The Data Governance System
Components of the Data Governance System:
1. Policy for data governance
2. Procedural controls
3. Technical controls
4. Data maps and data walks
5. Risk identification, ranking, and filtering
6. Data reviews
7. Data and operational audits
8. Employee awareness and training
9. Management oversight

Fig. 2: *Data Governance.*

- Laboratory building and facilities security and access control
- Facilities disaster recovery plan
- Analytical test method validation
- Verification of compendial procedures
- Electronic records and signatures
- Electronic records storage, backup, archival, and restoration
- General procedures for computer system validation
- Chromatographic data acquisition software
- Electronic laboratory notebooks (ELNs)
- Laboratory information management system (LIMS)
- Computer system change control procedures
- Validation of spreadsheets
- Validation of databases
- Power failure recovery procedures for computers
- Disaster recovery of electronic data and computer equipment
- Computer system integrity
- Operational maintenance of computer systems and software
- Overview of data governance and data integrity
- Data source and data mapping
- Application of hazard analysis critical control points (HACCPs) to laboratory data integrity
- Personnel compliance program for insuring laboratory data integrity
- Workflow, sample management, tracking, trending, and release of analytical data
- Analytical data review and approval
- Conducting, documenting, and reporting laboratory investigations, out-of-specification (OOS) and out-of-trend (OOT) investigations
- QA oversight and monitoring of production
- QA oversight and monitoring of QC laboratory operations

III. List technical controls, inherent within system hardware and software, to prevent or restrict users from unauthorized or inadvertent manipulation or deletion of data. Verification has to be through qualification or validation procedures. Technical controls are always preferable to procedural controls because they exclude or limit the manipulation or deletion of data or records. FDA recommendations emphasize the restriction on the ability to alter specifications, process parameters, data, or manufacturing or testing methods (for example, by limiting permissions to change settings or data).

BACK TO CONTENTS

IV. Description of processes to assess and evaluate existing controls over data. This is the generation of workflow diagrams of the production and testing steps during the manufacturing of the product (data maps). Data maps should be as comprehensive and detailed as possible to ensure that all risks to data integrity have been identified. After data mapping, it will be necessary to execute more detailed mapping exercises with the laboratory (data walks). Each QC instrument/testing process should be mapped to illustrate how data is created, modified, reported, and managed. Data walks can be used as a training program.

V. Risk identification, ranking, and filtering are performed through gap analyses and risk assessment tolls. The former includes all documentation of observed gaps with linkage to the steps in the data maps, and the latter used to be accomplished in numerous fashions. Table 1 shows an example of a risk ranking and filter (RRF) tool, which can be used to construct a data and operational audit program.

Table 1

C1 =	**Data Criticality** = Impact on decision making, product quality and patient safety, namely: (A) Does the data influence important decisions? (B) What is the impact of the data on product quality or patient safety?		

High = 10
Medium = 5
Low = 1
NA = 1			

R1=	**Risk to Data** = Susceptibility to unauthorized: (A) Alteration of data and records (B) Deletion of data and records		

High = 10
Medium = 5
Low = 1
NA = 1			

D1 =	**Detectability** = Likelihood of detection/visibility of changes, alterations or deletion of data and records with existing data integrity procedures and practices		
Easily Detected = 1 Might be Detected = 5 Difficult to Detect = 10 NA = 1			
F1=	**Frequency** = A qualitative (or if data is available, quantitative) sense of how often the observation or practice occurs within the organization over time: (A) Isolated incident (B) Periodically occurs (C) A Reoccurring issue		

Rarely = 1
Occasionally = 5
Frequently = 10
NA = 1			

	High Risk Score =	> 5000	Red
	Medium Risk Score =	Between 1000 and 5000	Yellow
	Low Risk Score =	< 1000	Green

Table 1: *An example of a risk ranking and filtering (RRF) tool.*

VI. Data review is a standard component of any cGMP laboratory and needs to be driven by SOP. There are three levels of data review:

- Bench level
- Supervisor/management level
- Quality assurance (QA)

VII. As mentioned earlier, a data and operational audit program; long-term and QA-led, could be implemented. Taking into account the risk assessment, this program could include:

- Identifying critical oversight points for quality assurance (QA-COP)
- Determining a required level of QA oversight
  Level 1: Routine compliance challenges
  Level 2: Minor compliance challenge
  Level 3: Major compliance challenge
  Level 4: Critical compliance challenge
  Level 5: Out-of-control compliance challenge
- Determining the type of oversight requires:
  - Samples and data review
  - Observation of execution of the individual tasks
  - Interview personnel who perform individual work tasks
  - Confirm the performance of work tasks
  - Challenge the operation of selected LCS sub-systems
  - Witness execution of compliance related to sub-systems
- Creating and implementing audit plans and integrating the audits into the regular, routine QA oversight function (Fig.3).

VIII. Enhancing employee awareness and training on the principles of data governance and data integrity is of paramount importance within pharmaceutical companies. The most effective manner to accomplish this is through direct management involvement. The following outline serves as a starting point for the management design of the data governance and data integrity training program. However, each organization must have its own unique requirements that suit its individual needs:

- History of data governance and data integrity in the pharmaceutical industry
- Regulations regarding data integrity
- Definition of data governance and data integrity
- Importance of data integrity
- Policy and procedures regarding data governance and data integrity
- Employee data integrity confidential reporting mechanisms
- Timelines and timing regarding data governance and data integrity instructions

IX. The FDA is very clear on management oversight of the data governance system and data integrity. Management at all levels must create and implement a quality culture to prevent lapses in data integrity. Some examples of steps or actions that management could take:

- Develop a functional understanding of the production system

BACK TO CONTENTS

Figure 3

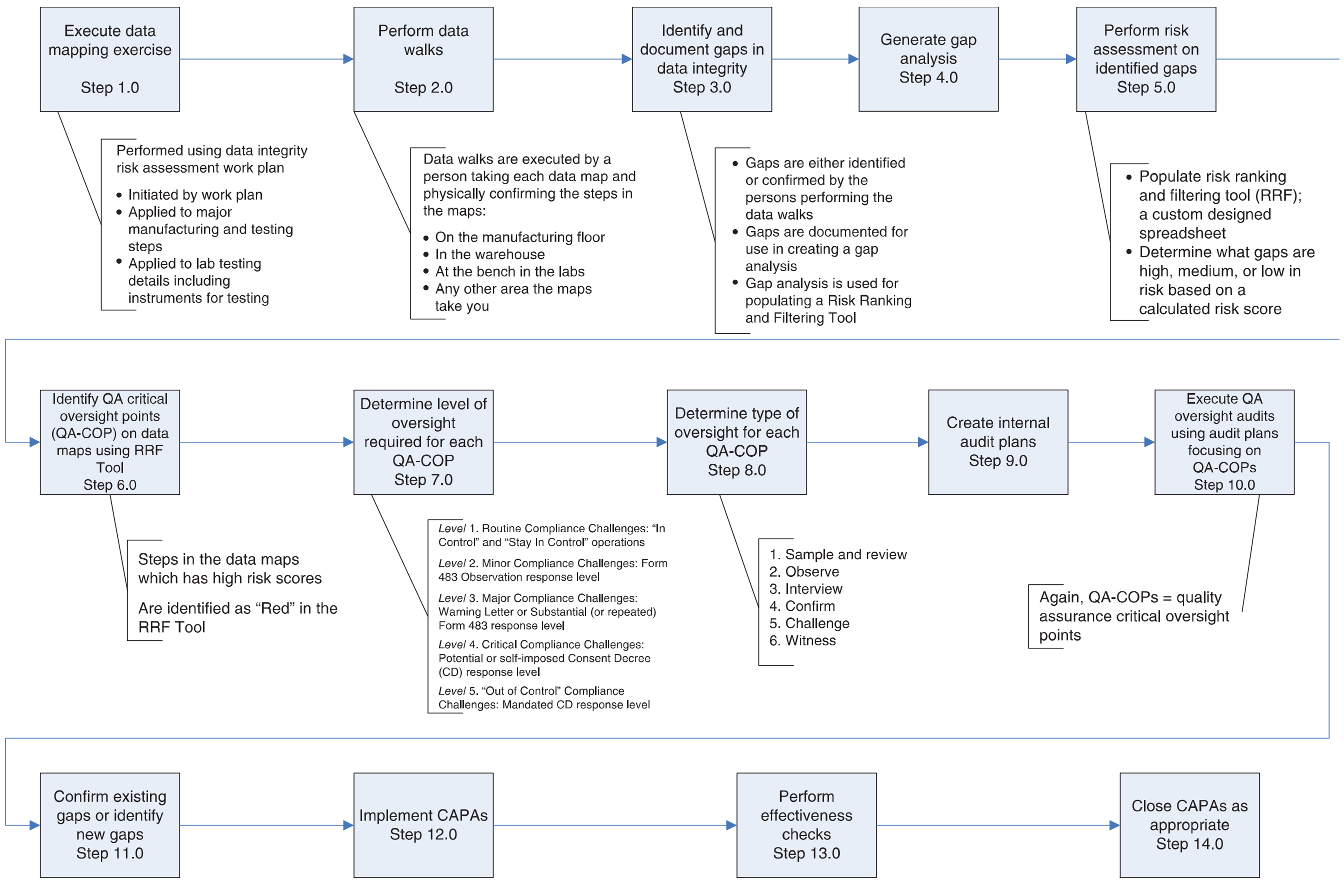

Execute data mapping exercise
Step 1.0
Perform data walks
Step 2.0
Identify and document gaps in data integrity
Step 3.0
Generate gap analysis
Step 4.0
Perform risk assessment on identified gaps
Step 5.0
Performed using data integrity risk assessment work plan
• Initiated by work plan
• Applied to major manufacturing and testing steps
• Applied to lab testing details including instruments for testing
Data walks are executed by a person taking each data map and physically confirming the steps in the maps:
• On the manufacturing floor
• In the warehouse
• At the bench in the labs
• Any other area the maps take you
• Gaps are either identified or confirmed by the persons performing the data walks
• Gaps are documented for use in creating a gap analysis
• Gap analysis is used for populating a Risk Ranking and Filtering Tool
• Populate risk ranking and filtering tool (RRF); a custom designed spreadsheet
• Determine what gaps are high, medium, or low in risk based on a calculated risk score
Identify QA critical oversight points (QA-COP) on data maps using RRF Tool
Step 6.0
Determine level of oversight required for each QA-COP
Step 7.0
Determine type of oversight for each QA-COP
Step 8.0
Create internal audit plans
Step 9.0
Execute QA oversight audits using audit plans focusing on QA-COPs
Step 10.0
Steps in the data maps which has high risk scores
Are identified as "Red" in the RRF Tool
Level 1. Routine Compliance Challenges: "In Control" and "Stay In Control" operations
Level 2. Minor Compliance Challenges: Form 483 Observation response level
Level 3. Major Compliance Challenges: Warning Letter or Substantial (or repeated) Form 483 response level
Level 4. Critical Compliance Challenges: Potential or self-imposed Consent Decree (CD) response level
Level 5. "Out of Control" Compliance Challenges: Mandated CD response level
1. Sample and review
2. Observe
3. Interview
4. Confirm
5. Challenge
6. Witness
Again, QA-COPs = quality assurance critical oversight points
Confirm existing gaps or identify new gaps
Step 11.0
Implement CAPAs
Step 12.0
Perform effectiveness checks
Step 13.0
Close CAPAs as appropriate
Step 14.0

Fig. 3: *Quality assurance data and operations audit program workflow.*

- Develop a functional understanding of the LCS
- Be aware of the balance between workloads, and the level of qualified and experienced staffing
- Be aware of the balance between workloads and the appropriateness of production and laboratory facilities and equipment
- Use the output from the data mapping and data walking to make corrective and preventive action plans
- Stay current with the most recent regulatory actions regarding data integrity
- Meet regularly with employees to train and discuss current trends related to data integrity
- Periodically visit the manufacturing floor and the laboratory bench
- Avoid counterproductive behavior, such as putting pressure on personnel to release a product, or making employees feel that mistakes will be held against them
- Understand cultural differences and norms in ethnically diverse work environments
- Establish a data integrity reporting system, which allows employees to anonymously report data integrity issues or concerns
- Ensure that the right number of the right people have the right tools and are working in the right environment that values their personal safety
- Stay engaged with QA

Tools & Templates

The templates are provided in an **electronic format**

Example-Template **Data Integrity Risk Assessment Work Plan**
Example-Template **Data Map for the Manufacture of a Drug Product**
Example-Template **A Generic Laboratory Instrument Data Map**
Example-Template **Gap Analysis for Manufacturing Steps**
Example-Template **Gap Analysis for a Laboratory Instrument Data Map**
Example-Template **Risk Ranking and Filter Tool**
Example-Template **Laboratory Data Flow for Notebook and Data Review**
Example-Template **Notebook and Data Review Checklist**
Example-Template **Quality Assurance Data and Operations Audit Program WorkFlow**

BACK TO CONTENTS

Glossary	
Audit Trail	A secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of an event relating to the creation, modification, or deletion of an electronic record.
Backup Files	An original copy of the original record that is maintained securely throughout the record retention period. Backup data must be complete, exact, and secure from alteration, inadvertent erasures, or loss
Data	Facts, figures, and statistics are collected together for references or analysis. All original records and original copies of the records including, source data and metadata and all subsequent transformation and reports of that data.
Data Criticality	May be determined by considering how the data is used to influence the decision made.
Data Governance	The sum total of arrangements to ensure that data, irrespective of the format in which is generated, recorded, processed, retained, and used ensures a complete, consistent, and accurate record throughout the data lifecycle.
Data Integrity	The extent to which all data are complete, consistent, and accurate throughout the data lifecycle.
Data Lifecycle	All phases in the life of the data, from the initial generation and recording through processing, use, data retention, archive, retrieval, and destruction. Facts, figures, and statistics are collected together for reference or analysis.
Data Processing	A sequence of operations performed on data to extract, present, or obtain information. In a defined format.
Data Risk	Represent the vulnerability to unauthorized deletion or alteration of data and the likelihood of detection during a routine review.
Dynamic Record	A record format that allows interaction between the record content and the users.
Electronic Signature	A signature in digital format that represents the person signing the document or record. Electronic signatures are legal equivalents of handwritten signatures.
Metadata	Metadata is the contextual information required to understand data and describes the attributes of other data and provides context and meaning.
Raw Data	Original records retain the format in which they were originally generated. Raw data must be contemporaneously and accurately recorded by permanent means.
Statics Records	A fixed-data document such as a paper record or electronic image allows little or no interaction between the user and the recorded content.

BACK TO CONTENTS

Data integrity within the biopharmaceutical sector in the era of Industry 4.0

Adapted from Alosert, H. *et al.* (2022)

Article

Product quality, safety, and efficacy are the biopharmaceutical industry´s main concerns when manufacturing therapeutics. Regulatory bodies need to review a significant amount of data to ensure good manufacturing practice (GMP) processes are robustly designed to consistently deliver high-quality, efficacious, and safe products to patients. Regulators expect all product quality results to also meet the necessary data integrity (DI) standards.

High throughput platforms, process analytical technologies (PAT) facilities, and better process-monitoring and control assure the improved quality of products. However, these innovations have significantly increased the amount and complexity of data generated during the manufacturing process. The need to extract information from such complex datasets has further reinforced the criticality of DI bioprocessing. Likewise, DI has been integral to the 4.0 industry development, which describes smart future factories that integrate autonomous real-time monitoring and control.

Therefore, there is a need to address the criticality of DI and how to mitigate any potential DI risk within manufacturing processes that follow the current GMP (cGMP).

DI standards

In 2013, the FDA introduced the ALCOA acronym to indicate that data must be attributable, legible, contemporaneous, original, and accurate, with the addition of being complete, consistent, enduring, and available, commonly referred to as ALCOA+. Implementing ALCOA+ can help to detect risks and avoid jeopardizing or delaying regulatory products' approval.

DI regulations and violations

In recent years, regulatory warning letters have risen, of which 43% feature DI issues. The guideline topics ranged from training staff on data processing to checking internal audit trails and validation control strategies. Common DI violations typically relate to data manipulation and falsification. This highlights the importance of sound scientific judgment needed to justify alterations made to restricted data and adhering to regulations on formal documents to record and modify procedures.

Manufacturing systems and DI – risks and mitigating measures

The international standard for control systems (ISA-95) was designed to define electronic information exchanged between manufacturing control functions and other enterprise functions as shown in figure 2.

Computerized systems pose some DI challenges. However, issues typically stem from inappropriate management of complex data records and failure to validate systems in use. As more computerized systems are used by biopharmaceutical manufacturing industries, there is a need to shift from a legacy paper-based approach to a fully electronic-based system to alleviate risks related to error-prone tasks and to streamline documentation.

Another method to reduce DI issues is through frequent internal audits and record reviews, which identify areas that fall short of DI compliance and enable mitigating measures.

Good, automated manufacturing practice (GAMP) was therefore established to provide a risk-based approach for achieving compliant GxP computerized systems in industries, which includes meeting DI regulations. It needs validated systems to generate the compliant data necessary for process monitoring and control. Different analytical systems store and generate data across different formats, this is one of the major limitations, and more work is required to standardize these data formats. On the other hand, datasets, pre-processing, and manipulation are required to produce readable results by an analyst. Recording metadata is of paramount importance as it captures the essence and purpose of the experiments and simplifies analysis.

Industry 4.0 – The impact of data analytics and smart manufacturing solutions on DI

Raw data must always be archived safely and made available for regulatory inspections during the validation period to ensure DI standards are met. That is why the data, and the method of storage, transfer, and processing must be verified and documented to assure that data accuracy and integrity are preserved.

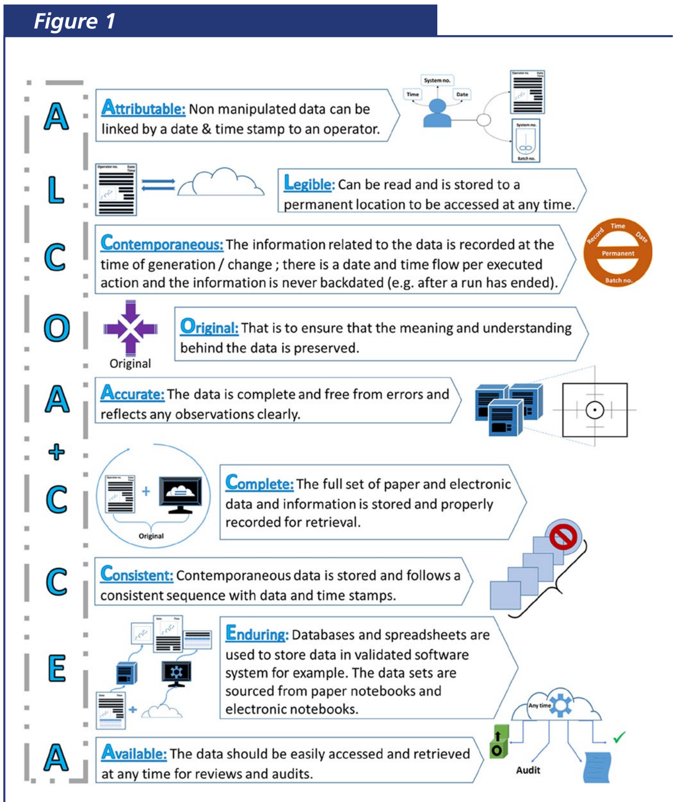
GMP environments would benefit from integrating the corrective and preventative action (CAPA) procedures, which must be designed to identify, investigate, and understand the root causes of issues.

Smart manufacturing solutions such as cloud platforms can increase security and accessibility, to safely store and transfer large complex data volumes onto a single server to preserve its DI throughout processing. Although, this poses risks related to data transfer, data ownership, and access, particularly in the context of global biopharmaceutical companies with multiples sites in various countries that are governed by different data compliance regulations. The challenge is the availability of a fast and secure network connection to achieve the required short latency time to offer real-time monitoring capabilities for effective monitoring and control. Figure 3 shows a summary and illustrates the solutions within industry 4.0 that meet DI standards.

Future measures to mitigate DI risks

Along with the digital maturation in the biopharmaceutical industry, measures to mitigate risks will be considered. Independent logins are suggested to function as identification signatures, even on shared systems to make the data attributable and traceable. Blockchain applications rely on multi-step verification of the data generated to ensure data traceability, transparency, and security. Another solution is internal auditing which helps track procedures, action plans, and control measures implemented to determine if there is a need for requalification or DI violations. Monitoring connections also are useful to track logins, helping to trace anomalies. An electronic batch record or laboratory information management (LIMS) system is recommended to automatically save electronic entries. In addition to all, the use of numbered and controlled forms for manual transcripts recorded on portable tablets can also assist with quality checks.

Figure 1



A – Attributable: Non manipulated data can be linked by a date & time stamp to an operator.

L – Legible: Can be read and is stored to a permanent location to be accessed at any time.

C – Contemporaneous: The information related to the data is recorded at the time of generation / change ; there is a date and time flow per executed action and the information is never backdated (e.g. after a run has ended).

O – Original: That is to ensure that the meaning and understanding behind the data is preserved.

A – Accurate: The data is complete and free from errors and reflects any observations clearly.

+

C – Complete: The full set of paper and electronic data and information is stored and properly recorded for retrieval.

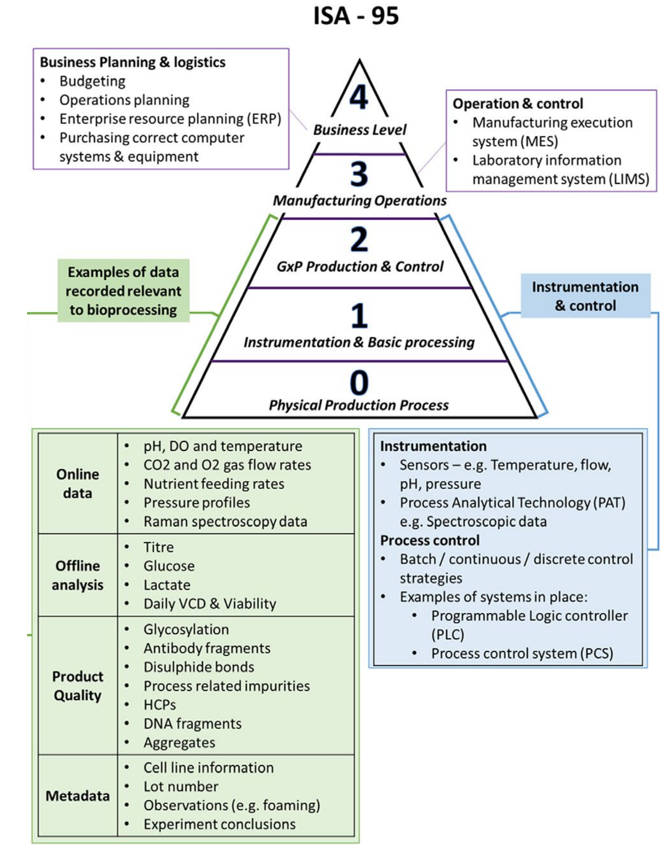
C – Consistent: Contemporaneous data is stored and follows a consistent sequence with data and time stamps.

E – Enduring: Databases and spreadsheets are used to store data in validated software system for example. The data sets are sourced from paper notebooks and electronic notebooks.

A – Available: The data should be easily accessed and retrieved at any time for reviews and audits.

Fig. 1: *FDA´s ALCOA+ description.*

Figure 2



ISA - 95

4 Business Level

3 Manufacturing Operations

2 GxP Production & Control

1 Instrumentation & Basic processing

0 Physical Production Process

Business Planning & logistics
- Budgeting
- Operations planning
- Enterprise resource planning (ERP)
- Purchasing correct computer systems & equipment

Operation & control
- Manufacturing execution system (MES)
- Laboratory information management system (LIMS)

Examples of data recorded relevant to bioprocessing

Online data	pH, DO and temperature CO2 and O2 gas flow rates Nutrient feeding rates Pressure profiles Raman spectroscopy data
Offline analysis	Titre Glucose Lactate Daily VCD & Viability
Product Quality	Glycosylation Antibody fragments Disulphide bonds Process related impurities HCPs DNA fragments Aggregates
Metadata	Cell line information Lot number Observations (e.g. foaming) Experiment conclusions

Instrumentation & control

Instrumentation
- Sensors – e.g. Temperature, flow, pH, pressure
- Process Analytical Technology (PAT) e.g. Spectroscopic data

Process control
- Batch / continuous / discrete control strategies
- Examples of systems in place:
  - Programmable Logic controller (PLC)
  - Process control system (PCS)

Fig. 2: *ISA-95 five-layer framework to computerized systems relevant to GMP bioprocess manufacturing.*

BACK TO CONTENTS

Figure 3

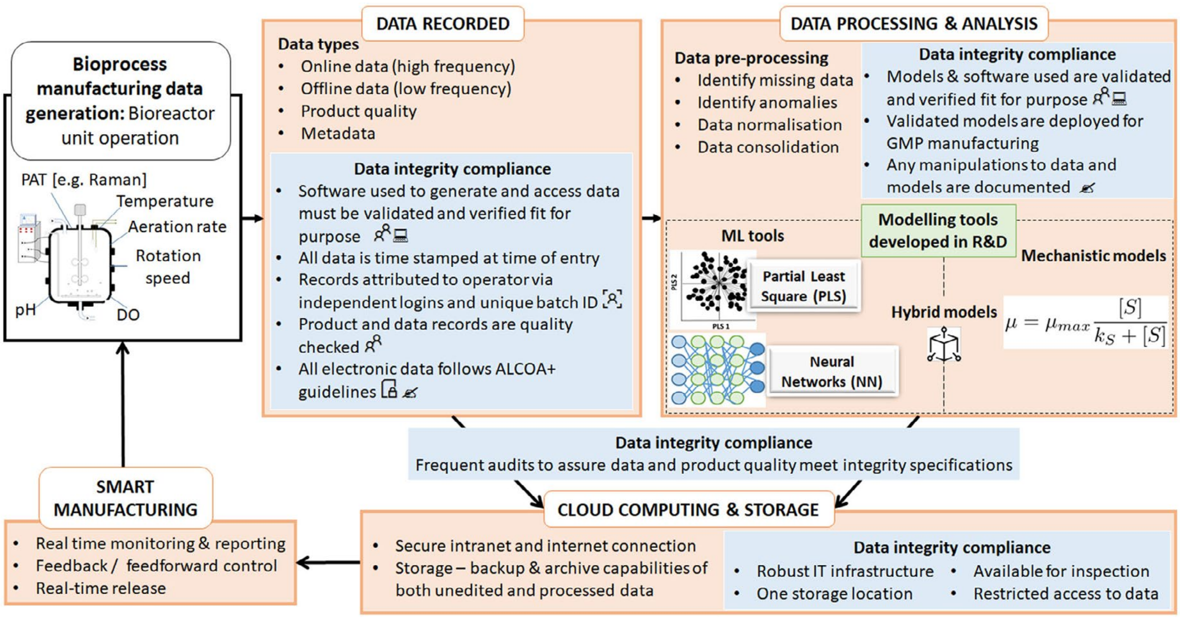

Bioprocess manufacturing data generation: Bioreactor unit operation
PAT [e.g. Raman]
Temperature
Aeration rate
Rotation speed
pH
DO
DATA RECORDED
Data types
• Online data (high frequency)
• Offline data (low frequency)
• Product quality
• Metadata
Data integrity compliance
• Software used to generate and access data must be validated and verified fit for purpose
• All data is time stamped at time of entry
• Records attributed to operator via independent logins and unique batch ID
• Product and data records are quality checked
• All electronic data follows ALCOA+ guidelines
DATA PROCESSING & ANALYSIS
Data pre-processing
• Identify missing data
• Identify anomalies
• Data normalisation
• Data consolidation
Data integrity compliance
• Models & software used are validated and verified fit for purpose
• Validated models are deployed for GMP manufacturing
• Any manipulations to data and models are documented
ML tools
Modelling tools developed in R&D
Mechanistic models
PLS 2
PLS 1
Partial Least Square (PLS)
Hybrid models
$\mu = \mu_{max}\frac{[S]}{k_S + [S]}$
Neural Networks (NN)
Data integrity compliance
Frequent audits to assure data and product quality meet integrity specifications
SMART MANUFACTURING
• Real time monitoring & reporting
• Feedback / feedforward control
• Real-time release
CLOUD COMPUTING & STORAGE
• Secure intranet and internet connection
• Storage – backup & archive capabilities of both unedited and processed data
Data integrity compliance
• Robust IT infrastructure
• One storage location
• Available for inspection
• Restricted access to data

Fig. 3: *Necessary steps required to ensure data integrity is mantained in an Industry 4.0 bioprocess throughout a data lifecycle specific to a bioreactor. This encompasses the advanced technologies using smart manufacturing approaches to record, process and produce compliant results for bioprocess monitoring and control.*

BACK TO CONTENTS

Ensuring data integrity of healthcare information in the era of digital health

Adapted from Zarour, M., *et al.* (2021)

Article

Data integrity, known as the way to ensure data quality, efficiency, and continuity throughout its lifecycle, is the most sensitive concern for the current healthcare industry. For better experience and fewer infrastructure requirements, each country is pursuing a digitalized healthcare sector. The objective of the present study is to investigate the different worldwide data integrity management systems through high-quality published papers.

Current trends in data integrity risk

Data breach situations in a worldwide scenario are a disaster for information security in the healthcare sector. Potential attacks illustrate that a data breach in the healthcare industry requires some guaranteed safeguards for the security of healthcare information or electronic medical records. In this context, one study shows that 85% of devices in medical organizations are using or running outdated operating systems or infrastructure, and this situation develops an open path for attackers to exploit vulnerabilities and effectively harm the healthcare sector.

According to an online survey conducted by HIPPA between 2009-2019, data breaches in the healthcare sector are at its worst, despite adequate safeguards against malware attacks. The HIPPA´s report cites 25 of the healthcare sector’s biggest data breaches in the last ten years. Authors classified the attack introduced most frequently in healthcare organizations with the aid of that record. The hacking of confidential information is the primary factor in the infringement of medical data. In addition to this, employees´ mistakes, incompetence, and suspicious insider activities are included. Healthcare attacks represent 62% of total information technologies (IT) incidents. In addition, 94% of healthcare organizations have reported cyber-attacks on their networks. The number of breaches increased thrice in 2018 compared to 2017.

A critical analysis of these attacks offers a clear condition of healthcare services’ data integrity.

Related works

Most of the studies and reports have addressed administrative characteristics and needs, and a few have explored different approaches to privacy and data protection. For this motive, the authors have pointed out that a systematic literature review (SLR) is needed to present strategies for data integrity and a guide to demonstrate the research activity in this field.

Literature examination

To conduct a literature analysis on this topic, the literature of relevant topics was analyzed and selected. SLR was performed through various scientific databases (PubMed, Google Scholar, Science Direct, IEEE Xplore, among others), using the following keywords: healthcare information security, electronic medical record security, healthcare data integrity, and medical data transfer, with the Boolean operator AND. Then inclusion/exclusion criteria were applied and a list of 20 reports was analyzed.

The inclusion criteria were defined as:

- Identify data integrity security concerns in healthcare and propose quantitative solutions
- A discussion of healthcare reputation using a particular approach
- Studies reported in Q1 and Q2 Journals
- Studies with some definitive evidence on healthcare credibility issues

While the exclusion criteria were:

- Articles that did not apply the

BACK TO CONTENTS

Figure 1

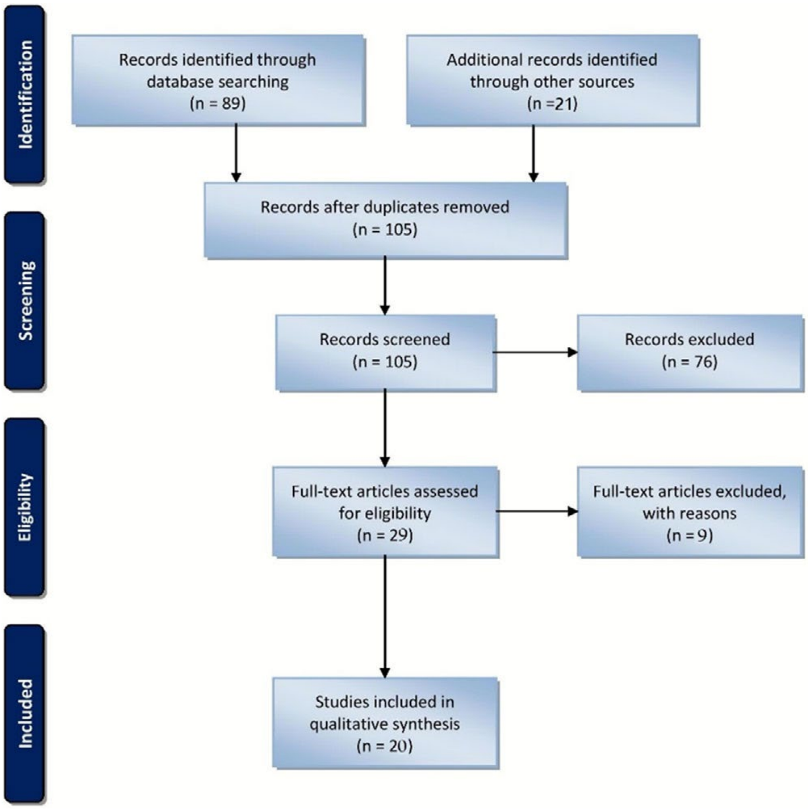

Identification
Records identified through database searching (n = 89)
Additional records identified through other sources (n =21)
Records after duplicates removed (n = 105)
Screening
Records screened (n = 105)
Records excluded (n = 76)
Eligibility
Full-text articles assessed for eligibility (n = 29)
Full-text articles excluded, with reasons (n = 9)
Included
Studies included in qualitative synthesis (n = 20)

***Fig. 1:** Flowchart of the report selection.*

conditions of the request and the examination intention

- Articles that addressed data integrity but not from the view of healthcare
- Records that are not accurate and definitive to support the healthcare problem of data integrity

Exploratory analysis of results

Selected articles were classified according to the method of data integrity used during the study.

- 5 of the 20 studies selected analyzed blockchain technology to securely manage healthcare data
- 8 of the 20 studies published articles on the security enhancement of patient data in connected medical devices via masked authenticated messaging extension.

This SLR also analyzed facets of the healthcare platform for data integrity protection and that way, the current analysis that the healthcare record integrity must be improved via multiple management strategies for the entire healthcare system.

To understand which methodology of data integrity was given greater interest, the result shows a major interest in computer science. In addition, paper quartiles demonstrate that the standard of research work is quite useful in data integrity strategies of healthcare, as there is a lack of information in this area.

A Fuzzy-AHP procedure was conducted between the selected articles. This analytical tool is used to make decisions analyzing a multi-criteria problem. It takes a pairwise comparison of different alternatives respective to various criteria and provides a decision support tool. The result of this analysis corroborates that the investigators must concentrate on blockchain technology for good solutions to maintain data integrity.

Conclusion

This SLR offers an overview of the current situation for healthcare data integrity. The results strongly indicate that this sector needs a new and more robust data integrity approach.

Table 2

Author	Study description	Technique for data integrity
William J Gordon *et al.* (2018) **Read**	The study describes how to facilitate the blockchain approach in the healthcare sector. The paper also discusses the challenges that are associated with blockchain to provide secure communication.	Blockchain
James Brogan *et al.* (2018) **Read**	The study provides distributed ledger technologies in advancing electronic health information. The paper provides a cost-effective and novel approach for healthcare organizations.	Masked authenticated messaging extension
Peng Zhang *et al.* (2018) **Read**	The paper provides a blockchain-based architecture FHIR-chain for securing medicare.	Blockchain
Christian Esposito *et al.* (2018) **Read**	The study uses a cloud storage environment for data available in healthcare organizations and for patients. Authors also use a blockchain approach for secure lab report transactions and communication.	Blockchain
Prosanta Gope *et al.* (2020) **Read**	The study uses a body sensor network approach for facilitating secure and integrity-managed architecture of IoT in healthcare.	Secure-BSN
Pasupathy Vimalachandran *et al.* (2017) **Read**	The authors proposed an authorization-based model for Australian healthcare services.	Authentication
Mohamed Elhoseny *et al.* (2018) **Read**	The study provided a stenographic technique with hybrid encryption mechanism for securing health records and images.	Encryption
Entao Luo *et al.* (2018) **Read**	The study provides a secure sharing-based data transfer in IoT environment for data security of healthcare organizations.	Slepian-Wolf Coding-based Secret Sharing Scheme (SW-SSS)
Moshaddique Al Ameen *et al.* (2012) **Read**	The paper discusses the challenges and issues associated with the wireless sensors in the healthcare sector.	-
Gunasekaran Manogaran *et al.* (2017) **Read**	The authors give a secure organizational IoT-based model for storing and processing wearable sensor data in medical services.	Secure Cloud
Benjamin Fabian *et al.* (2015) **Read**	The study provides inter-organizational data transfer security through various security attributes. The paper provides the architecture for secure data transfer from one organization to another.	Secure Cloud
Jinyuan Sun *et al.* (2011) **Read**	The paper provides a secure health record system for patient privacy based on cryptographic techniques and IoT environment of the healthcare industry.	Cryptography
Abdullah Al Omar *et al.* (2017) **Read**	The study presents a data management system for healthcare services to facilitate patients through blockchain technology.	Blockchain
Sue Bowman (2013) **Read**	The study highlights the current challenges and error causes in healthcare data integrity in healthcare organizations. The paper also provides a review of the current HER system of healthcare.	-
Anastasia Theodouli *et al.* (2018) **Read**	The study presents a mechanism for facilitating blockchain technology for providing auditable and sharable data in healthcare organizations.	Blockchain
Mohammad Zarour *et al.* (2020) **Read**	The study used a hybrid fuzzy-based methodology for evaluating the impact of different blockchain technology models in a healthcare perspective.	Blockchain
Karim Abouelmehdi *et al.* (2018) **Read**	In this study, the authors have discussed the challenges and survey the current situation of healthcare big data.	-
Anam Sajid *et al.* (2016) **Read**	The study presents a review of healthcare medical data security for providing privacy to patients. The paper also discusses the currently used techniques and approaches in the healthcare system.	-
Brihat Sharma *et al.* (2018) **Read**	The study proposes a model, the Merkle tree-based approach to secure the integrity of health records. The software model closely refers to Blockchain technology.	Merkle tree-based approach
Katharine Gammon (2018) **Read**	The article illustrates blockchain application in the healthcare sector in various domains.	-

Table 2: *List and exploratory analysis of the selected reports.*

BACK TO CONTENTS

Digitalization in laboratories of the pharmaceutical industry

Adapted from Picker, T.S., (2021)

Article

Pharma 4.0 is defined as pharmaceutical production based on Industry 4.0, whereas Industry 4.0 describes digitalization as the fourth industrial revolution. The vision of the derived Laboratory 4.0 is visibility, transparency, prognosis, and adaptability.

The findable, accessible, interoperable, and reusable (FAIR) data principles describe the requirements of suitable data management. However, in the real world, laboratories demonstrated outdated ineffective manual processes or disconnected systems.

An analysis of the workflow of major companies identified five key processes to improve:

- Data collection
- Availability of data
- Automated data flow
- Centralized master data management
- Integrated migration management

Table 1 lists common processes in the laboratory and the possible IT solution.

Motivation for digitalization in the laboratory

Staff expectations

Good scientific practice requires easy access and safe data recording and storing. In the world of plug-and-play, devices without automated and continuous data flow are no longer accepted. The "digital natives" will no longer spend time in unnecessary manual processes.

Increasing throughput

Smart processes without manual processes and system discontinuity are needed to decrease the effort per experiment (throughput time). This can lead to an increase in sample throughput and gives time for creative work on new experiments.

Repeatability

Bearing in mind the customary practice of reporting results but keeping the raw data on the devices, repeatability might be improved by the inclusion of this information in the data analysis.

Enhanced requirements in data integrity

These requirements are the ones described in the ALCOA+ principles. Compliance defined by the authorities seems to be impossible without further digitalization.
A: attributable
L: legible
C: contemporaneous
O: original:
A: accurate
+: complete, consistent, enduring, and available.

Centralized archiving

In an environment without an integrated data flow and centralized storage of all relevant data, the implementation of a more automated and monitored central archiving is worth the higher initial investment due to less operation effort and a lower risk of data loss.

Ad hoc analysis

Shared access is simplified as data are stored in a standardized format. Another advantage of standardized and centralized access routines is that cumbersome familiarization with specific software is not needed. If the data-sharing workflow is well implemented and optimized, data are available for distribution to functional experts shortly after recording. Sharing data requires responsible handling and interpretation. A lack of sufficient expertise of understanding the data or a lack of statistical knowledge may lead to the misinterpretation of results.

The value of data

The main argument for increasing digitalization is the potential value of the collected data. Limited access rights comprise additional internal efforts or missing external knowledge about the metadata. New responsibilities and processes need to be established, such as the responsibility of the data creator to store the data following the FAIR principles and the responsibilities of the data user to correctly use it and communicate with the creator. Digitalization in laboratory processes will help to collect structured data with high information density.

Table 1

Tasks	Explaination	IT systems, examples
Search for initial information	• Define objective • Search for available information in in-house and external libraries, databases • Ideation	• Electronic laboratory notebook (ELN) • SciFinder, Scopus, Espacenet, online search tools (Bing, Google [Scholar], Cambridge crystallographic database, crystallography open database, ELN, books, and journals [electronic, websites of publishers]) • Mind mapping, video conferencing
Set-up experiments	• Purchase chemicals, glassware, equipment • Educate and train staff • Codify, i.e. name experiments and samples	• Web shops, catalogs • eLearning, videos, supplier demo • Registration system, label printer
Design	• Calculate system properties (e.g. $\mathrm{p}K_A$, solubility, crystal structures) • Define range and details for experiments • Estimate and prospect progress (e.g. mixing, heat transfer)	• In silico prediction tools • Design of experiments (DoE) • Simulation tools (e.g.computational fluid dynamics [CFD], process modeling)
Execute/control experiments	• Program electronic equipment (heating/cooling, dosing, stirring), define profiles • Sampling and process analytics (timing, actions, measures, e.g. temperature, pH, pressure, particle size [distribution], concentration)	• (Semi)automated lab reactors • Process analytical technologies (PAT) (sensors, probes)
Document process recipes	• Planned parameters and methods vs. • Executed parameters and methods • Data integrity	• Lab devices, electronic lab notebook (ELN), lab execution systems (LES), lab information management system (LIMS)
Document chemical analytics (observations, results)	• Data retrieved from sampling and process analytics (at-, in-, off-line) • Ensure data integrity (ALCOA+)	• Lab devices, electronic lab notebook (ELN), lab execution systems (LES), lab information management system (LIMS) • Scientific data management systems (SDMS)
Process and analyze the data	• Data tidying (if necessary) • Understand the data and relations • Transform to knowledge • Derive conclusions (result or set up further experiments)	• Self-made macros, processing • Machine Learning (statistics, uni-, multivariate analysis, clustering) • Visualization (charts, video, animation) • Automated processing • Artificial intelligence (AI) (i.e. self-training/self-improving algorithms)
Reporting	• Summarize, communicate, and explain results • Consider different type of addressees • Level of detail, e.g. operators, supervisors, project team (CMC, core team), management, customers • Functional experts, e.g. synthesis, solid state, analytic, formulation, marketing, regulatory, patents • Purposes, e.g. internal vs. external publication, functional expert vs. layman	• Reporting tools • Text processor, presentation tools, Wikis, corporate databases • Automated processing • Aggregation • Visualization
Distribute data	• Submission • Further analysis	• Corporate data collections • Data mining (big data, smart data) • Artificial intelligence (AI) • Frameworks

Table 1: *Solid-state laboratory processes supported by IT solutions.*

Figure 1

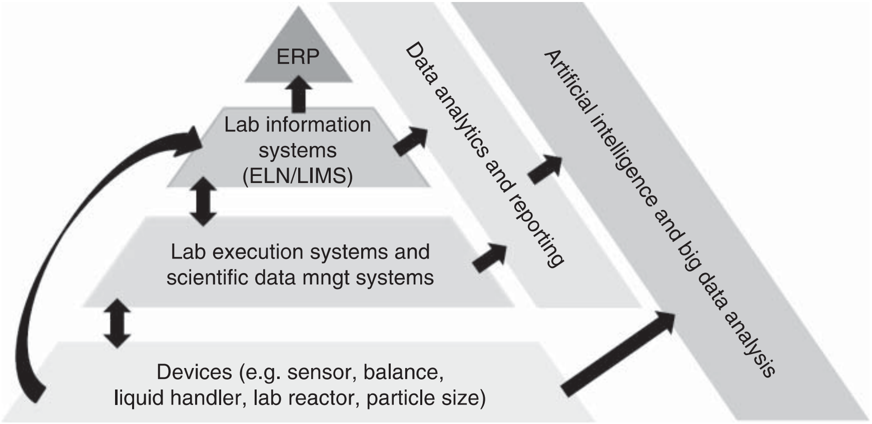

ERP
Lab information systems (ELN/LIMS)
Lab execution systems and scientific data mngt systems
Devices (e.g. sensor, balance, liquid handler, lab reactor, particle size)
Data analytics and reporting
Artificial intelligence and big data analysis

Fig. 1: *Hierarchical categories of laboratory information system. ERP: enterprise resource planning; ELN: electronic lab notebook; LIMS: lab information management system.*

Categories of laboratory IT systems

Devices

Devices have the highest number of entities. This group comprises a wide range of instruments, from simple sensors to complex equipment and creates two-dimensional data. In addition to the required data formats for import and export, adapters and interfaces of the device should be considered.

Lab Execution Systems (LES) and Scientific Data Management Systems (SDMS)

This group is the second layer of IT solution for controlling the complexity of experiments processing and the collection of recorded data. Consumers usually select the best in all hierarchical levels of devices and IT solutions and expect universal connectivity. Multi-manufactured and multi-brand solutions appear more future-oriented and will quite likely be the system of choice if flexible implementation and operation are sought.

Lab data system

This is involved in nearly every action of the laboratory and can be divided into the sample-based LIMS and the experiment-based ELN. LIMS are used in analytical laboratories that analyze a high number of samples and few experiments. On the other hand, ELNs are better fulfilled in laboratories with a higher number of different systematic methods and fewer samples.

Enterprise resource planning (ERP)

This is a single, centralized system for the production, planning, and recording of relevant economic data. Another advantage is the compliant storage and handling of quality-related data such as batch recording.

Figure 2

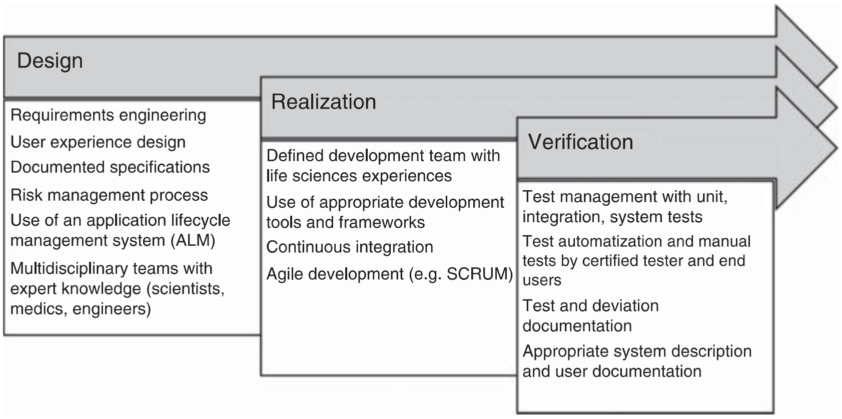

Design
Requirements engineering
User experience design
Documented specifications
Risk management process
Use of an application lifecycle management system (ALM)
Multidisciplinary teams with expert knowledge (scientists, medics, engineers)
Realization
Defined development team with life sciences experiences
Use of appropriate development tools and frameworks
Continuous integration
Agile development (e.g. SCRUM)
Verification
Test management with unit, integration, system tests
Test automatization and manual tests by certified tester and end users
Test and deviation documentation
Appropriate system description and user documentation

Fig. 2: *Recommended software development process based on general GAMP principle.*

In case of any collection between the output of the laboratory and the patients or any influence on information used for the submission, the relevant guidance documents need to be respected (good manufacturing practice and good medical practice).

Further use of data

Data analysis and reporting: this solution can integrate several sources and apply the provided methods and reports to the results of several devices and systems. Open-source solutions, such as R or KNIME, allow the use of state-of-art methods for statistics, graphic presentation, or data manipulation into data science workflow, supported by an easy-to-use graphical user interface. Open-source solutions are also available for single or periodical reporting in predefined formats.

Big data analytics and artificial intelligence: in addition to ad-hoc analysis, the more comprehensive data analytics uses systematical approaches to gain new knowledge from the existing data. In pharmaceutical laboratories, the additional services provided by data analytics and artificial intelligence (AI) can be used to optimize processes and products.

System interfaces for data exchange

One of the most mentioned hurdles towards the digital transformation of laboratories is the missing standardization of interfaces.

Adapters

The physical gateway of the system enables laboratory instruments to communicate with each other at the same or different hierarchical levels. The most common adapters in the industry are serial port (RS232), universal serial bus (USB), ethernet, and cable-less connection (such as Wi-Fi and Bluetooth)

Communication medium and protocols

The exchange of information needs a medium and detailed rules. Limiting the diverse ways of communication in a laboratory and use of international standards facilitate data exchange. Some examples are file-based communication, ANSI/ISA-88 batch control (S-88), open platform communication unified architecture (OPC UA), and standard in lab automation (SiLA)

Data formats

Devices produce data in individual file formats. To implement the FAIR data principles, a central data format is recommended. The common data formats, such as TXT, XML, or JSON could be used, as well as the analytical information markup language (AnIML, based in a common xml format), allotrope data format [ADF, based on hierarchical data format (HDF)].

Implementation of IT solutions

Each implementation starts with the selection of the project and the general project setup.

Identification of digital gaps in the lab processes

To find the best topic for the next digitalization project, companies follow different strategies. Here is a description of different examples:

- Contextual inquiry: the method consists of the observation of users, accompanied by detailed questions. It is particularly suitable for the identification and understanding of the most cumbersome and error-prone data processes in the environment of the key personnel in the laboratory. It allows the selection of worthwhile areas in which to improve support with IT solutions.
- Interaction room (IR): To align interdisciplinary teams and enhance the communication between IT experts and subject matter specialists, a workshop in the IR could be useful for determining a business model, analyzing the touchpoints between customers and sample examination, and observing the life cycle of a sample or the data that describe the process.

Implementation approach

Regardless of the regulatory obligations, it is worth considering in all software implementation projects if following the principles of the validation process is advised. In this context, it might be useful to use a specialized solution for application lifecycle management (ALM). This solution enables the structured and linked documentation of all development-related artifacts like requirements, specifications, risks, codes, and tests with enhanced possibilities of completeness check, reporting, and change management of the single item. Figure 2 summarizes recommendations for a software development process based on general good, automated manufacturing practice (GAMP) principles.

Conclusion

Implementation of appropriate standards and IT solutions to replace manual processes will help to reduce the risk of transmission errors and free up resources for innovative research.

BACK TO CONTENTS

The story behind a game-changing collaboration in accurate titration

Björn Christensen reveals how Metrohm and Sartorius teamed up to create a simple, secure, and fully integrated titration system.

The new Metrohm platform, OMNIS, brings together all of Metrohm´s analytical techniques into one embedded software platform that can interact with other platforms. This combination is based on what is missing in each company: in Sartorius a software platform and Metrohm physical parameter determination equipment.

In this case, the team set out to create a complete titration system. First, they had to set a sample size, as when dealing with solids, most of the time they must be weighed. Weighing is an important parameter. The OMNIS platform has integrated software and technologies but does not have a balance. Therefore, they made a complete integration with the Sartorius Cubis II balance.

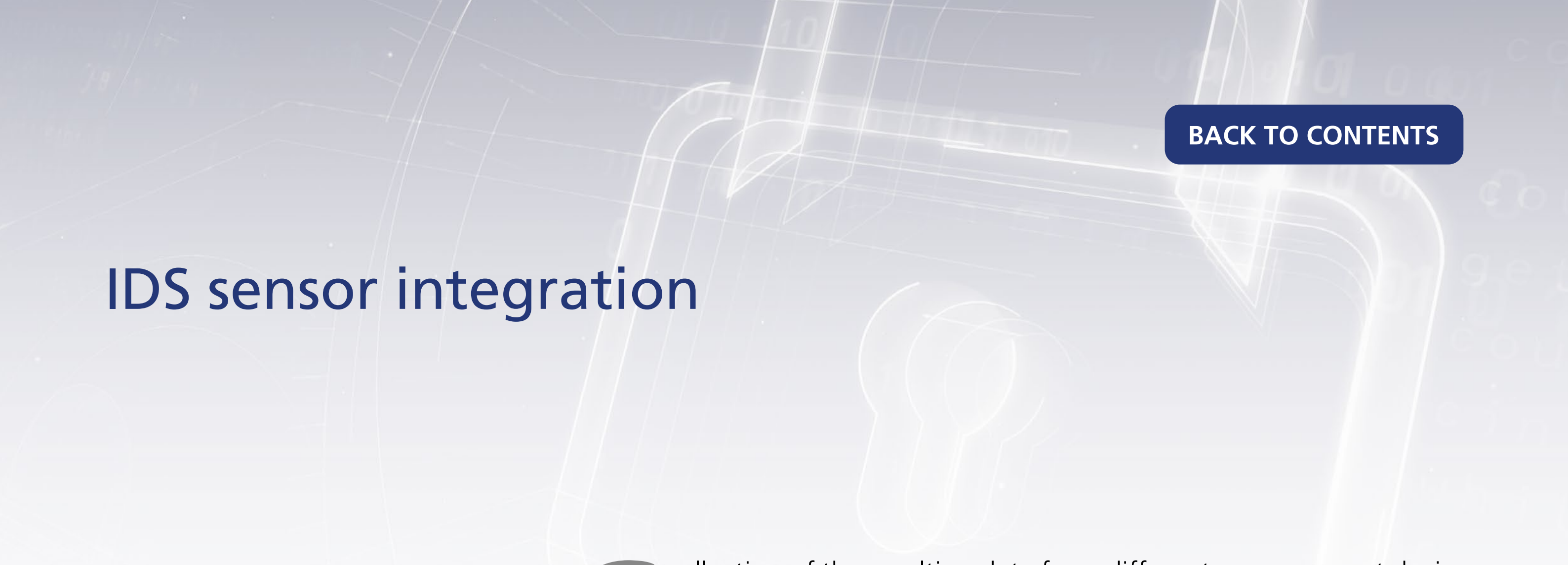
Through an application called QApp you can set up and have the option to work under full compliance hand in hand with OMNIS software. You can access all available OMNIS clients and decide which client you would like to connect with. You log in on the balance screen with credentials from OMNIS. The communication is both encrypted and secure and has a functionality that recognizes normal devices from Metrohm or OMNIS. The weighing in or weighing out of a sample, or a complete sample series, can be edited directly from the balance, without the need to start OMNIS. Tolerance limits regarding sample weight can be graphically represented on the display of the balance and, if there are several OMNIS clients within the same network, they can share the same Cubis II balance.

This integration has many benefits, such as keeping the measuring unit consistent and editing from the balance terminal. Request or back-weighing can also be carried out directly from the balance. The balance can be remote-controlled by OMNIS for other processes. One of the best things about the integration of these technologies into one working platform, is that is easy to use, no matter what your level of experience is.

This helps to keep up with ever-increasing regulations set by governing bodies, such as the FDA. This integrated system does not allow values to be changed without being recorded. The process is monitored in the software and stored in an audit trail. When integrated with the local network, encryption of any data exchange ensures that the highest standards of data integrity and security are always met. All the weighing information is stored in OMNIS, so you do not need an audit trail for the balance.

The three main key standouts of this system are workflow integration, a central administration, and the highest standards in terms of data security and data integrity.

BACK TO CONTENTS



IDS sensor integration

Collection of the resulting data from different measurement devices is typically handwritten, sent to a laboratory printer or transferred. These approaches rarely fulfill all data integrity requirements. A further challenge with integrating laboratory equipment directly into a computerized system is the absence of an industrial standard that meets compliance requirements. Another difficulty is inconsistent handling when changing from the computerized system to the laboratory equipment within a workflow.

Sartorius and Xylem Analytics have developed a solution, allowing easy integration of Cubis II balances and IDS measuring sensors, creating a customized laboratory workflow with a plug-and-play connection via recognized IT standards, and offering sufficient protection against data integrity problems.

This IDS system is equipped with a plug-in head and attachable universal radio modules. Cubis II can connect to these wireless sensors, receive the measurement and metadata, and present results on its display. The user can enter a sample ID for a measured value via the onscreen keyboard or a barcode scanner. IDs can also be retrieved from a LIMS system via web services. The measured value can be recorded directly or together with associated weighing values and documented as compliant through various electronic or paper-based options.

A QApp workflow can monitor critical process parameters and calculate, evaluate, and record results automatically. IDS sensors can also be integrated into the workflow to record and process their measured values together with the weighing results.

The results can be automatically transferred to a LIMS or documented electronically in PDF/CSV format or paper based. This interaction minimizes errors, simplifies documentation, and increases process speed.

Cubis II offers a wide range of options for both compliant paper-based and compliant electronic recording of measured values whether these come from the IDS sensor or the balance itself. This integration adheres to ALCOA documentation principles to meet regulatory requirements. The results and related metadata are shown directly on the balance display, where they can also be marked as an invalid event of incorrect recordings. The user must confirm the generated report with their electronic signature.

This solution is designed to provide all necessary technical controls for compliant use, such as role-based user management with optional LDAP integration or audit trail for regulatory compliance.

BACK TO CONTENTS

Integration of Sartorius Cubis II premium balances into Starlims from Abbott Informatics

The problem with integrating laboratory equipment into a computerized system is the absence of an industrial standard that meets all compliance requirements, as well as the no-consistent handling when changing from the computerized system to the laboratory equipment inside a laboratory workflow.

Sartorius has developed Cubis II, the first series of lab balances to feature a completely modular design. This concept lets you create a customized profile for your specific app requirements. Cubis II has become the benchmark to use in regulated sectors that impose the highest requirements, such as global pharmaceutical labs.

On the other hand, Abbot Informatics´ Starlims improves the reliability of laboratory sampling processes, supports compliance with global regulatory requirements and industry standards, and provides comprehensive reporting, monitoring, and analysis capabilities. Communication between the client and the server is achieved through standard web services messaging over hypertext transfer protocol (HTTP) or optional secure (S-HTTP), for a more protective environment. Each Cubis scale is an independent unit that can communicate over RESTWeb Services Starlims. To read and verify sample identification tags, a hand scanner that can read different types of matrix codes can be connected directly to the Cubis II. The Cubis II QApp allows the integration of laboratory workflow. The application can be customized to meet the customer's SOPs to 100% and must be validated, resulting in both greatly reduced cost and risk for the end customer.

The workflow implementation starts in Starlims. The samples are created and assigned to the analytical method and a specific Cubis II balance. The samples are labeled with a barcode that contains the sample ID from Starlims to track them during the whole process. The user logs onto the Cubis II with their personal login and scans samples with the barcode reader. The balance verifies directly that the scanned sample is included in the sample list and that the logged-in user is allowed to work with this sample. The user is guided step by step through the weighing process on the display of the balance. This protects against the incorrect operation, improper use, or violation of the weighing-related SOP. Cubis II sends the weighing result together with all required metadata to Starlims, automatically calculates the difference between the initial and residual weights and stores the raw data securely. The full integration of Cubis II into Starlims guarantees no manual data handling, data integrity over the entire lifecycle, device monitoring, calibration, and personal user account, which prevents the unauthorized use of the system. In addition, the user is guided and monitored step by step through the whole process, which ensures that SOPs and business rules are being followed.

BACK TO CONTENTS

Interview with Holger Densow Product Specialist at Sartorius

Holger Densow studied biology at the University of Bielefeld, Germany, and finished his Doctorate in 2005. He worked as a sales representative for 2.5 years at a German biotech company and in 2008 switched to another company to manage lab instruments as a Product Manager. Since 2016 he is a Product Manager at Sartorius and is responsible for software solutions for lab balances.

Why are connectivity and compliance so important in today's lab environment?

The challenge is the reproducibility and integrity of results. With manual data transfer unintended or intended falsification of results can happen. For research laboratories that is a question of the publication of results and the application for new funding. With retracted papers, the creditability is damaged, and it is hardly possible to apply for new grants. For industrial laboratories, especially in the pharmaceutical industry, the business can be severely affected by omitting compliance. In the worst case, a company is banned from a market and cannot sell its products any longer.

What challenges do labs face today when it comes to balances, connectivity, and compliance?

In general, the key issue concerning the digitalization of laboratories is the missing standardization of communication protocols or the use of proprietary middleware solutions. The connection of laboratory instruments to databases such as LIMS/ELN/MES systems is not an out-of-the-box plug-and-play solution. The integration and communication between these system-specific connectors must be developed. The integration costs are only covered by laboratories that are forced to follow specific rules or guidelines for example 21 CFR part 11. Other laboratories avoid these costs and very often still rely on written paper records. Although digitalization is desirable for almost all laboratories the development and maintenance costs and a lack of IT expertise prevent many laboratories from going digital.

What is Cubis-II?

Cubis-II is a configurable balance offering thousands of hard- & software combinations and superior weighing performance. The motto is "You only pay for what you need." Concerning software options, the special focus is on connectivity and compliance. The software package "Pharma" and "Connectivity" offer technical controls for 21 CFR part 11 & USP chapter 41/Ph. Eur. chapter 2.1.7 compliance, and safe & reliable direct data transfer to SMB, FTP, or other servers.

How does Cubis-II address the need for connectivity and compliance in labs today?

Cubis-II addresses the topic of compliance and connectivity in many ways. The software package Pharma offers tools and applications for 21 CFR part 11 compliance and compliance to USP and Ph. Eur., and the software package Connectivity connects to servers, databases, or specialist data mining solutions. Following the ALCOA principles, data integrity is maintained, and easy integration into the lab IT infrastructure by versatile direct connectivity options are given.

How does Cubis-II set itself apart/differentiate itself from other balances on the market?

The flexibility to configure the balance as required and the versatile communication protocols make the integration of the balance into the existing IT infrastructure as easy as possible. Cubis-II does not rely on proprietary middleware solutions but instead can directly export data to data storage systems like file servers and LIMS. Files are sent with a checksum that is recorded in the balance audit trail and by comparing the exported checksum file with the checksum recorded in the audit trail data integrity can be verified.

How cost-effective is the process compared to the former techniques?

I would rather compare the costs with other solutions. With Cubis-II, direct data transfer to third-party software solutions like LIMS/ELN/MES systems is possible. Sartorius does not use middleware with limited options for the integration of third-party instruments. Existing middleware solutions create licensing and maintenance costs whereas, once established, the connectivity solutions of Cubis-II balances create no additional costs.

BACK TO CONTENTS

Imprint

© Wiley-VCH GmbH
Boschstr. 12,
69469 Weinheim,
Germany
Email: info@wiley-vch.de

Editors:
Róisín Murtagh & Birgit Foltas

Senior Account Manager:
Jan Käppler

Sartorius Lab Instruments GmbH & Co. Kg
Otto-Brenner-Str. 20,
37079 Goettingen,
Germany

Cover: © 2022 Adobe Stock