DASSAULT SYSTEMES

BIOVIA

HOW TO ADDRESS YOUR DATA INTEGRITY PROGRAM

White Paper

INTRODUCTION

The regulatory focus on Data Integrity has significantly increased over the past two years and is highlighted by the number of regulatory guidance documents issued by the UK MHRA, US FDA, World Health Organization (WHO), China FDA (CFDA), Pharmaceutical Inspection Cooperation Scheme (PIC/S), Therapeutic Goods Authority (Australia) and other regulatory authorities around the world. A comparison of the UK, US and WHO guidance below, demonstrates that regulators are largely focused on the same issues and controls requirements.

TOPIC	US FDA	UK MHRA	WHO
Definitions	✓	✓	✓
Data Governance Strategy, Training, Whistle-Blower Policy/Practice	✓	✓	✓
Design of Processes and Systems (locations/scribes)		✓	✓
Raw Data, Meta Data, Original Records and True Copies Control	✓	✓	✓
Control of QC Testing and Results	✓		
Primary and Subordinate Records Control		✓	
Control of Blank Forms (Paper records)	✓		✓
Data Review (including Exclusion of Data and Audit Trail Review)	✓	✓	✓
Data Retention – Archival, Backup Copies	✓	✓	✓
Computerized Systems Validation and Electronic Record, Signatures	✓	✓	✓
Audit Trails Requirements	✓	✓	✓
Computerized Systems Access Control	✓	✓	✓
Data Integrity Issue Remediation Approach	✓		✓

Regulatory guidance does not establish any new regulations, rather it reinforces the need to comply with existing GxPs in protecting data supporting decisions relating to product quality and patient safety. Data Integrity requirements are illustrated in US FDA Parts 211 and 212 which include:

- **§211.68** (requiring that "backup data are exact and complete," and "secure from alteration, inadvertent erasures, or loss");
- **§212.110(b)** (requiring that data be "stored to prevent deterioration or loss");
- **§211.100 and 211.160** (requiring that certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound");
- **§211.180** (requiring that records be retained as "original records," "true copies," or other "accurate reproductions of the original records"); and
- **§211.188, 211.194, and 212.60(g)** (requiring "complete information," "complete data derived from all tests," "complete record of all data," and "complete records of all tests performed").

From a European Perspective, EU GMPs state:

- "…entries made in clear indelible handwriting…."
- "[alterations]…signed and dated….permit reading of original….reason recorded"
- " …records completed at the time each action taken…"
- "…accuracy of records should be checked…"
- "…name of persons carrying out activities…"

Given that Data Integrity regulation has existed for many years, why do we still have a problem today? Further, organizations significantly invested in the implementation of USFDA 21 CFR Part 11; Electronic Records; Electronic Signatures in the late 1990's which was intended to protect regulated electronic records against inadvertent or unauthorized change.

There may be many factors contributing to today's Data Integrity problems including:

- Lack of understanding of importance of data
- Lack of data ownership
- Outdated controls applied to new technologies
- Outdated technologies that do not provide adequate control
- Business pressures to do more work with fewer resources
- Lack of quality culture and open issues reporting
- Loss of subject matter experts
- Outsourcing of key activities

David Churchward of the UK MHRA shared inspection data from 2015 inspections at the ISPE conference in Barcelona, 2016. The inspection trend indicated that Data Integrity continues to be a major concern. UK MHRA inspection findings (Dosage form inspections Jan-Oct 2015) found that:

- 35% EU 'statements of non-compliance' for Data Integrity
  - 121 Major, 218 Other deficiencies had references relevant to Data Integrity
  - 20 Major Data Integrity deficiencies in regulatory action cases
  - 10 Major Data Integrity deficiencies under compliance management

At the ISPE Data Integrity Workshops, Bethesda, June 2016, Sarah Barkow of the US FDA indicated that between January 2015 and May 2016, 21 of the 28 Warning Letters issued by the US FDA contained Data Integrity citations.

CORE PRINCIPLES OF DATA INTEGRITY

ALCOA++

Data has integrity when it has ALCOA++ characteristics:

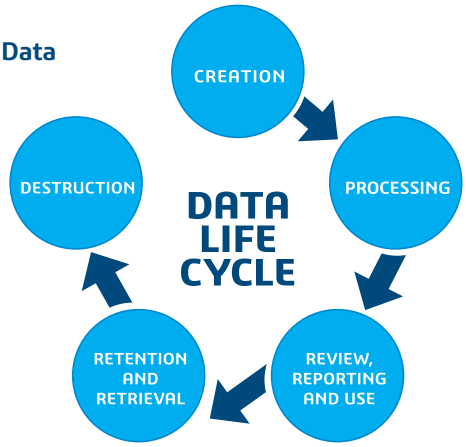
A	Attributable	All actions that create, modify or delete GxP records are attributable to an individual
L	Legible	Data must be readable, and unobscured by changes
C	Contemporaneous	Data must be recorded at the time the work is performed
O	Original	Data must be either an original record or a true copy
A	Accurate	Data accuracy must be controlled to eliminate errors and data changes must be documented
+	Complete	All data pertaining to a GxP record shall be retained as part of that record
+	Consistent	Data, its meta data and sequential timestamps must be consistent
+	Enduring	Data must be recorded in a durable medium and must be readable for as long as it is retained
+	Available	Data must be available and accessible for its whole retention period

A combination of processes and technologies ensure that data has the ALCOA++ attributes throughout its life. Internal review and audit processes shall ensure that data has these attributes.

DATA LIFECYCLE

Data must be managed throughout its life. As such, appropriate controls must be applied to minimise the risk to data at each point in the lifecycle. It is good practice to map the data lifecycle which may be created, stored and processed by multiple computerized systems and manual processes throughout its life.

ISPE GAMP® Records and Data Integrity Guideline – Data Lifecycle



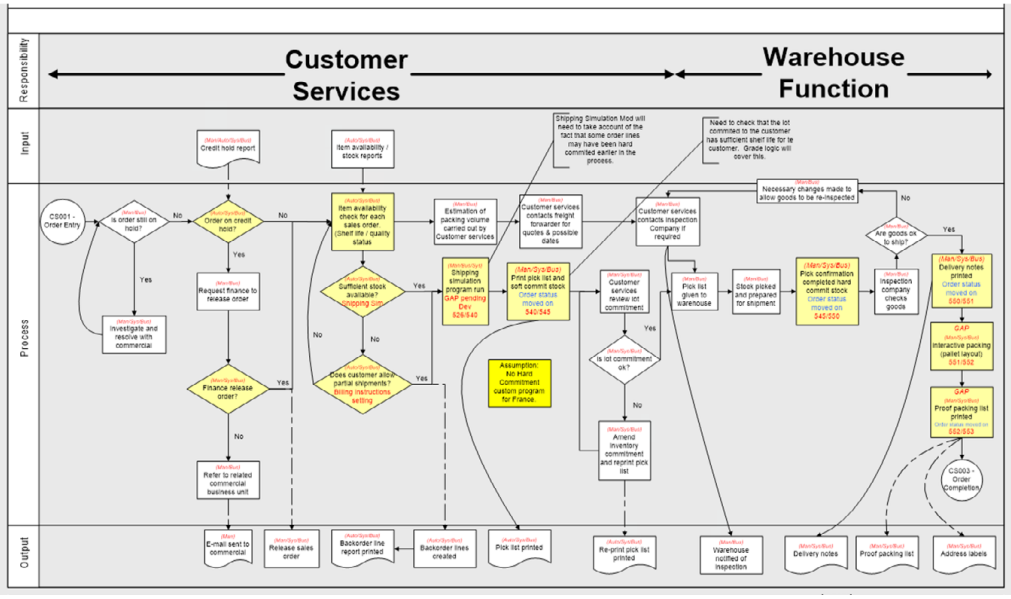
Risk assessments conducted against the data lifecycle determine the vulnerability to unauthorized or inadvertent access, change or deletion. Considerations in the risk assessment include:

- Use of data
- Protection of data
- Data transformation
- Data transfers
- Traceability of data transactions
- Data review
- Data approval

Examples of Data Integrity risks at various stages of the data lifecycle includes but is not limited to:

LIFECYCLE	EXAMPLE RISKS	EXAMPLE CONTROLS
Create	Secure format and storage Access authorisation Attributability Out of Specification	Accessibility User Access Management and Role Based Security Audit Trail and Unique User Accounts Data entry validation
Processing	Accuracy Incorrect processing Access authorization Inaccurate or incomplete transformation / transmission of results	Accuracy design User Access Management and Role Based Security Data Conversion and Migration Management / Data Buffering on interface failure
Review, Reporting and Use	Omission of results Over summarising results No visible audit trails No consideration of "just in specification" results Access authorisation	Data review Validation
Retention and Retrieval	Not retained for required period Accessibility and reprocessing capability of archived records	Archive and retrieval process / Data Conversion / Migration
Destruction	More a data privacy / legal concern rather than GxP	N/A

Mapping your business processes and identifying key data inputs and outputs during the process will ensure that data flows are clear and the use of data for GxP decision making is clearly understood.



The ISPE GAMP® Business Process and Electronic Records Risk Assessment processes are applied to determine the risk to Data Integrity based on the criticality of data, vulnerability of data and ability to detect unauthorized changes.

DATA INTEGRITY PROGRAM

Objectives and Scope

The primary objectives of the Data Integrity program are to establish:

- Knowledge of Data Integrity requirements across the organization
- Roles and responsibilities for management of data across the organization
- Required controls for management of paper and electronic GxP data / records
- An open culture for reporting, investigating and remediating Data Integrity issues

Data Integrity programs will address records in all formats, whether that is paper, electronic or other formats. Data Integrity programs also cover all GxP domains (Good Laboratory Practice, Good Clinical Practice, Good Manufacturing Practice, Good Distribution Practice and Good Pharmacovigilance Practice).

The Data Integrity program engages all business functions and regions supporting GxP operations. As such, it is essential that the Data Integrity program has executive sponsorship and is fully resourced and prioritized against other company initiatives.

Quality Management System

The outcome of the Data Integrity program will result in roles and responsibilities and processes that are an existing part of the Quality Management System. Data Integrity is no different to any other quality system requirement and must be integral to the daily operations of a regulated company.

Education

A global training program should be established to raise awareness and develop knowledge. Such training programs should be tailored to the audience. For example, some audiences will not respond to training that purely quotes regulatory requirements. Training should ensure that those operating business processes support clinical, laboratory, manufacturing, supply chain and vigilence processes understand the importance of data they are managing and the consequencies of failure to ensure Data Integrity. Training should further ensure understanding of the requirements to protect data throughout its lifecycle and the potential vulberabilities (risks) to data.

Automation

Process automation has a significant role to play in the protection of electronic records and data through:

- Enforcing adherence to business processes
- Provide process repeatability
- Validate data entry in accordance with business rules
- Ensuring that only authorized users operate business processes and interact with records / data
- Protect records and data against inadvertent or unauthorized access
- Provide traceability of user actions
- Ensure backup of records / data to minimize risk of loss
- Manage the exchange of records and data between systems
- Optimise the number of data sources

Current technology supports automation with process workflow capabilities, signature workflows and audit trails. Electronic solutions also provide the opportunity to integrate different systems in a seamless way ensuring Data Integrity and allowing easy data transfer and sharing within the organization and with supply partners. A comprehensive business platform with standard interfaces minimize validation efforts and support the availability of data throughout the value chain.

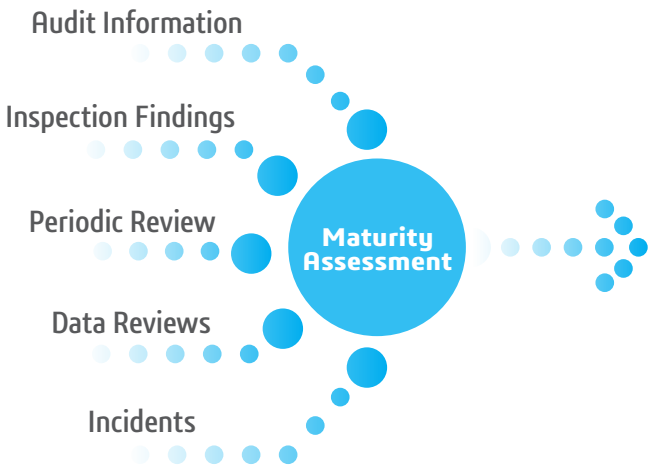
Determining the Effort

Technical controls alone do not assure Data Integrity. The Data Integrity program needs to address quality culture, governance, processes and technologies to engender the required behaviours as well as minimising the opportunity for Data Integrity issues.

To this end, it is important that your company's Data Integrity program is focused on the root cause of your Data Integrity problems rather than simply assessing the adequacy of process and technical controls. Indications of root cause or risk can be determined by analysing information that will be already available to your organization. Such information includes:

- Internal QA audits
- External regulatory inspections
- Deviation reports
- General observations
- IT issue / incident reports
- Periodic reviews
- Anecdotal evidence

Further, an indication of potential Data Integrity risks can be quickly obtained by conducting process / data orientated Data Integrity audits. Audits should go into the laboratory or production areas to observe operations. This is the easiest way to determine whether USB storage devices are plugged into Laboratory PCs, whether methods are copied and modified prior to execution, whether records are exported to Microsoft Excel® and manipulated prior to being included in the batch record.

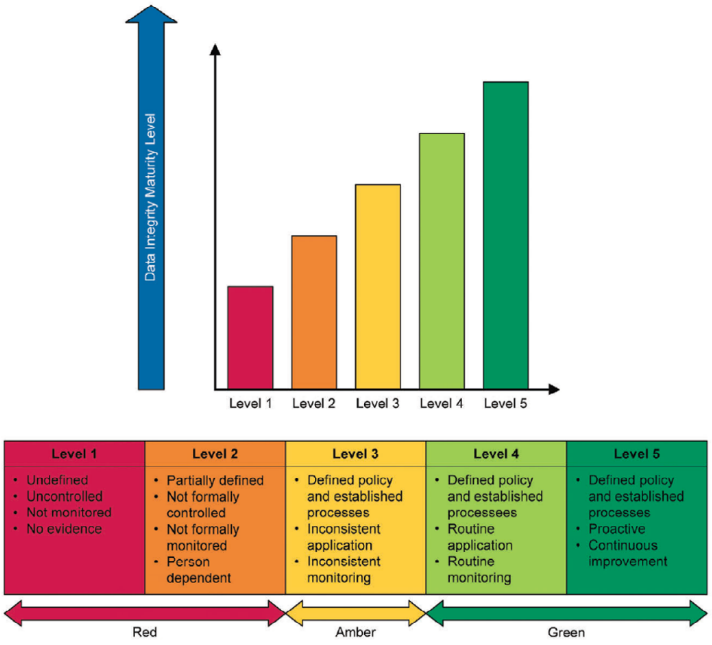


The table below shows some examples of Data Integrity indicators. As can be seen, the indicators are largely focused on knowledge and culture rather than a lack of technology controls. Addressing technical controls will minimise the opportunity for Data Integrity failures but will not address the motivation for falsification of data.

SCENARIO	UNDERSTANDING OF DATA	CULTURE / LEADERSHIP	PROCESS	TECHNOLOGY
I know the data isn't correct, but we must go live on Friday?	■	■	■	
Great training, but what does patient safety have to do with IS?	■			
I found a backdoor where I can access product data.				■
I re-wrote the record because the original was messy.		■		
I had to sign this record, but the quality of the scan is poor, and I can't read the data.	■	■		
It was easier to give him firefighter access than assign a role based on least privilege.	■	■	■	

Maturity Assessments

The GAMP Records and Data Integrity Guideline promotes maturity assessments to evaluate a company's controls maturity and to provide a benchmark for continuous improvement.



ISPE GAMP Records and Data Integrity Guideline – Maturity Assessment

The ISPE GAMP Records and Data Integrity Guideline provides guidance for the assessment of maturity in the areas of:

- Organization Culture
- Governance
- Strategic Planning and Data Integrity Program
- Regulatory
- Data Lifecycle
- Data Lifecycle Support Processes

A corporate Data Integrity program will conduct maturity across multiple locations, functions and cultures. It is essential that the results from such assessments are reliable and consistent across the organization. Disparity can occur due to:

- Cultural differences in reporting deficiencies
- Different perspectives on risk tolerance
- Different knowledge levels
- Different assessment methodologies

The corporate Data Integrity program must ensure that assessment outputs are "normalized". This can be achieved by ensuring:

- Data Integrity Subject Matter Experts (or Champions) are established across the organization
- Training is provided to ensure consistent knowledge
- Open reporting of issues is encouraged by management at all levels
- A consistent maturity assessment approach is established
- Knowledge is shared across assessment teams e.g. examples of assessments, risk examples, maturity level definitions
- Assessments are reviewed by a core team early in the program

Plans should be established to address significant issues and risks. There are several quick wins that can be implemented to improve Data Integrity. Some examples include:

QUICK WIN	DESCRIPTION
Establish Data Integrity Policy	Covers acceptable and unacceptable behaviours, definition of data to be controlled, key controls to be established, open reporting culture for Data Integrity issues
Training	Requirements of policy, Data Integrity risks (paper and electronic), understanding of "complete" data, roles and responsibilities for Data Integrity, expectations for managing Data Integrity
Leadership	Ensure controls established with Quality Management System, establish roles for ownership and management of GxP data, promote reporting of Data Integrity risks and issues, review Data Integrity risks and issues as part of risk management process, sponsor remediation of significant Data Integrity risks
Standard Controls	Establish standard user requirements / policies / standards for new systems / technologies including security and record protection and traceability controls
Automation	Enable available system controls including security features and audit trail capabilities.
Security	Review role based security profiles to ensure that access is based on least privilege and that access roles are appropriate to a user's business responsibilities.
Data Review	Implement enhanced data review processes that ensure that reviews identify: • Unauthorized processing of data • Modification of parameters prior to and during processing • Repeated processing of data without justification • Results trending close to the specification limits • Data has not been omitted from the results

SUPPLY PARTNERS

The development, manufacture and supply of safe pharmaceutical products is dependent on many supply partners. A Data Integrity failure within a supply partner organization may manifest itself in the products that your organization supplies. As such, it is essential that supply partners have relevant controls in place to manage Data Integrity. Quality Agreements with supply partners should include Data Integrity controls requirements. Audit and review processes should ensure that Data Integrity controls are understood and applied throughout the supply chain as, the marketing authorisation holder is ultimately accountable for Data Integrity.

SUMMARY

Data Integrity relates to all GxP records whether they are paper based, electronic or otherwise. Organizations must take a holistic approach that addresses the root cause of Data Integrity issues, this could be quality culture, leadership, processes or technology related. Most issues reported by industry regulators are related by the behaviour of organizations or individuals within organizations.

Technology provides an important means of reducing the risk of Data Integrity issues through the integration of systems, automation of manual processes, security of data and verification of data input / output and processing.

Prior to starting a corporate Data Integrity program, ensure that there is appropriate sponsorship from senior management and that the program focuses in the most critical areas. These areas can be identified from existing data derived from internal audits, reviews, external inspections, periodic reviews, deviations and Corrective Action / Preventive Actions (CAPA).

Although regulations are focused on regulated data and records, the principles of Data Integrity apply to all data / records / information managed within our organizations. The benefits of a robust Data Integrity program can equally relate to corporate Data Governance that effectively manages all aspects of business data and application of risk based controls.

For more information relating to Data Integrity, obtain a copy of the ISPE GAMP® Records and Data Integrity Guideline from https://www.ispe.org/publications/guidance-documents

REFERENCES

1. Data Churchward, UK MHRA, Presentation ISPE Barcelona Conference, 2016
2. Sarah Barkow, US FDA, International Society for Pharmaceutical Engineering Data Integrity Workshop June 5, 2016 Bethesda, MD - "Current Expectations and Guidance, including Data Integrity and Compliance With CGMP"
3. ISPE GAMP®, Records and Data Integrity Guideline, 2017
4. Mike Rutherford, Eli Lilly, Implementing a Corporate Data Integrity Program, Presentation ISPE Brazil, 2017
5. United States because it was solely created by NASA. NASA copyright policy states that "NASA material is not protected by copyright unless noted.

CHRIS REID

Chris is the Director/Principal Consultant at Integrity Solutions Ltd specialising in Business, Process Control, Laboratory and IT Systems. He was a key contributor to the development of GAMP 5 and a variety of GAMP® Good Practice Guides and is a member of ISPE's International Board of Directors.

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

Dassault Systèmes Corporate
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

BIOVIA Corporate Americas
BIOVIA
5005 Wateridge Vista Drive,
San Diego, CA
92121
USA

BIOVIA Corporate Europe
BIOVIA
334 Cambridge Science Park,
Cambridge CB4 0WN
England