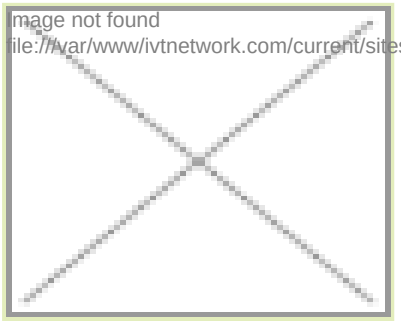
IVT NETWORK
Published on *IVT Network* (http://www.ivtnetwork.com)

# The Effective Use of CAPA When Things Go Wrong with Data Integrity

By **Ivan Soto  Apr 25, 2017 11:07 am PDT**




**Ivan Soto speaking on this subject at Data Integrity EU on 28-30 March, 2017.**

## INTRODUCTION

The industry continues to struggle to understand, implement and define a data integrity strategic direction. Several data integrity guidance documents have been published in recent years which create an additional level of complexity. Companies are struggling to understand which data integrity guidances are applicable to their business and how to align with the requirements defined in those documents.

This article will define data integrity, discuss myths and facts, and address challenges and the effective use of CAPA to remediate and close issues and gaps. This article will also provide clarity and understanding about how to define a strategy to ensure alignment with current data integrity requirements.

## DATA INTEGRITY: MYTHS & FACTS

Due to the amount of confusion related to data integrity, some companies are having delays in the implementation of critical electronic systems. Some of these delays are created by project team members that raise general high level data integrity concerns. Some of these concerns include:

- Does this system meet Annex 11 data integrity requirements?
- Does this system meets MHRA data integrity requirements?
- Does this system meets FDA data integrity requirements?

These may appear to be good questions but they provide little value because they are high level and fail to identify the specific areas of concern related to data integrity.

The lack of knowledge and clear understanding of data integrity requirements often lead to assumptions that have a negative impact on projects.

Some of these assumptions include the following:

- Electronic systems can **change data by themselves** and impact data integrity
- Data integrity is **only applicable to electronic records**
- Annex 11 is the driver behind data integrity requirements
- Data integrity requirements are **not applicable to paper-based records**
- If we have a **hybrid system, then we don't need to comply with data integrity requirements**
- We must perform audit trail reviews daily for all systems

All assumptions are driven by the lack of a knowledge of the requirements, which then leads to them being overanalyzed. Thus, project delays, higher implementation cost, and negative business impact are likely to occur.

Data integrity is not a new concern for the industry and the fact is that data integrity requirements are found in predicate rule requirements. The following facts are often not well understood by the industry:

- The biggest threat to data integrity is **PEOPLE**
- Data integrity is **not a new regulatory requirement**
- Data integrity is **applicable to both paper-based electronic records**
- Annex 11 is one driver behind data integrity requirements
- Data integrity requirements include both technical and procedural controls

Data integrity is considered a fundamental aspect of the quality system and a critical regulatory requirement for the industry.

**DATA INTEGRITY SHORTFALLS & CHALLENGES**

One of the biggest challenges facing the industry is the lack of a clear understanding about data integrity requirements. This leads to companies not understanding and knowing their data integrity gaps and issues. All these issues are key indicators of a lack of a data integrity strategic direction.

In some companies, data integrity becomes a philosophical debate between uninformed individuals who at best, have a vague understanding about data integrity.

Companies need to develop processes and procedures to minimize unncessary risks that can have a negative impact on data integrity. To do so, it is critical to understand factors that can compromise data integrity such as:

- Human errors when data is entered
- Errors that occur when data is transmitted from one computer to another
- Software bugs or viruses
- Hardware malfunctions, such as disk crashes
- Natural disasters, such as fires and floods
- Lack of adequate security
- Inadequate audit trails
- No audit trails available in the system
- Inadequate and inefficient audit trails periodic review process

From January 2014 – September 2015, over 25 data integrity related warning letters were issued to companies.

Some of the warning letters included the following:

- Failure to maintain complete data for all laboratory test performed
- Failure to implement adequate controls over electronic systems
- Failure to record activities at the time they are performed

**HOW TO IDENTIFY DATA INTEGRITY GAPS**

To identify data integrity gaps, companies need to understand their applicable regulatory requirements. The following questions need to be answered to define a strategic direction:

- Does the company need to comply only with FDA?
- Does the company need to comply with FDA, MHRA and Annex 11?

Once the company has identified their applicable requirements, they need to define a data integrity strategic direction.

When creating a data integrity strategic direction, one should consider:

- Creating an inventory of electronic systems in your facility
- Defining a Data Governance System
- Creating Gap Assessment Tools
- Performing gap assessments
- Drafting a remediation plan
- Creating CAPA's to address Gaps
- Forming a remediation summary report
- Closing all CAPA's

Having a data governance system is an MHRA expectation, as defined in their guidance document in March 2015.

MHRA defines a data governance system as:

"The sum total of arrangements to ensure that data, irrespective of its format in which it is generated, is recorded, processed, retained, and used to ensure a complete, consistent and accurate record throughout the data lifecycle."

To implement a data governance system that meets MHRA requirements, companies must implement processes and procedures that:

- Address data ownership throughout the lifecycle
- Consider the design, operation, and monitoring of processes/systems to comply with the principles of data integrity
- Feature controls over intentional and unintentional changes to information
- Promote staff training about the importance of data integrity principles
- Include relevant policies and procedures
- Take in mind the efforts and resources applied to organizational and technical controls of the data lifecycle element (they should be commensurate with it in terms of impact to product quality attributes)
- Create a working environment that encourages an open reporting culture of errors, omissions, and aberrant results
- Hold responsibility to senior management for the implementation and procedures to minimize potential data integrity risk

- Regulatory observations
- Internal audits
- Gap assessments

It is highly recommended that companies do not wait for a regulatory observation or internal audit to identify their data integrity gaps.

Companies should perform data integrity gap assessments against their applicable regulatory requirements. The gap assessments enable the ability to identify existing data integrity gaps. Gap assessments provide a structured approach to identify and document data integrity gaps. They also provide documented objective evidence to regulatory agencies about a company intent to comply with data integrity requirements.

Prior to performing gap assessments, companies need to identify their applicable data integrity regulatory requirements. Once the applicable requirements are identified, companies need to create a gap assessment tool.

The gap assessment tool should identify each individual data integrity requirement and document which procedures or records provide evidence of alignment. If a gap is identified, it must be documented in the tool and a target completion data should be defined. Remediation activities should be also documented in the gap assessment tool.

CAPA's must be created in the QMS to manage, track, and close all gaps identified during the gap assessment.

Data integrity CAPA's provide significant advantages and enable:

- Adequate tracking
- Closure by due date
- Quality approval
- Completion of all remediation activities

Data integrity gap assessments should be performed by a cross-functional team which should include the system owner, quality staff, and SME's such as engineering and IT.

The following deliverables should be created during the data integrity gap assessments:

- Gap Assessment Tool
- Data Integrity Remediation Plan
- CAPA's
- Data Integrity Summary Report

To effectively remediate and close out all data integrity gaps, companies need to manage the following challenges:

- Lack of organizational commitment

- Lack of resource commitment
- Downplaying the requirements
- Challenging CAPA’s
- Audit trail periodic reviews
- User access periodic reviews

Audit trail periodic reviews of CAPA’s can be challenging and may require a financial investment to remediate systems to meet the requirements.

It is highly recommended that for audit trails, remediation companies consider:

- Performing assessment of status quo
- Developing an understanding of the adequacy of legacy systems audit trails
- Defining the level of frequency based on system risk and product impact
- Creating child CAPA’s to remediate existing audit trail gaps

Audit trail remediation activities can be complex and costly for legacy systems that don’t meet current data integrity requirements.

**SUMMARY**

To enable compliance with data integrity requirements, companies must clearly understand their applicable regulatory requirements.

Understanding the specific applicable areas of data integrity enables companies to define a strategic direction for data integrity compliance.

To enable alignment with data integrity requirements, companies must understand the challenges and perform gap assessments to identify areas that need corrective actions.

Performing documented gap assessments, creating remediation plans and CAPA’s provide a structured approach to identify gaps, and corrective actions enable complete alignment with MHRA data integrity requirements.

---