SIVAND SANAT

Data Integrity in Pharmaceutical Industry: From Concept to Practical Requirements

8-Sep-2026

By: Hamed Benam



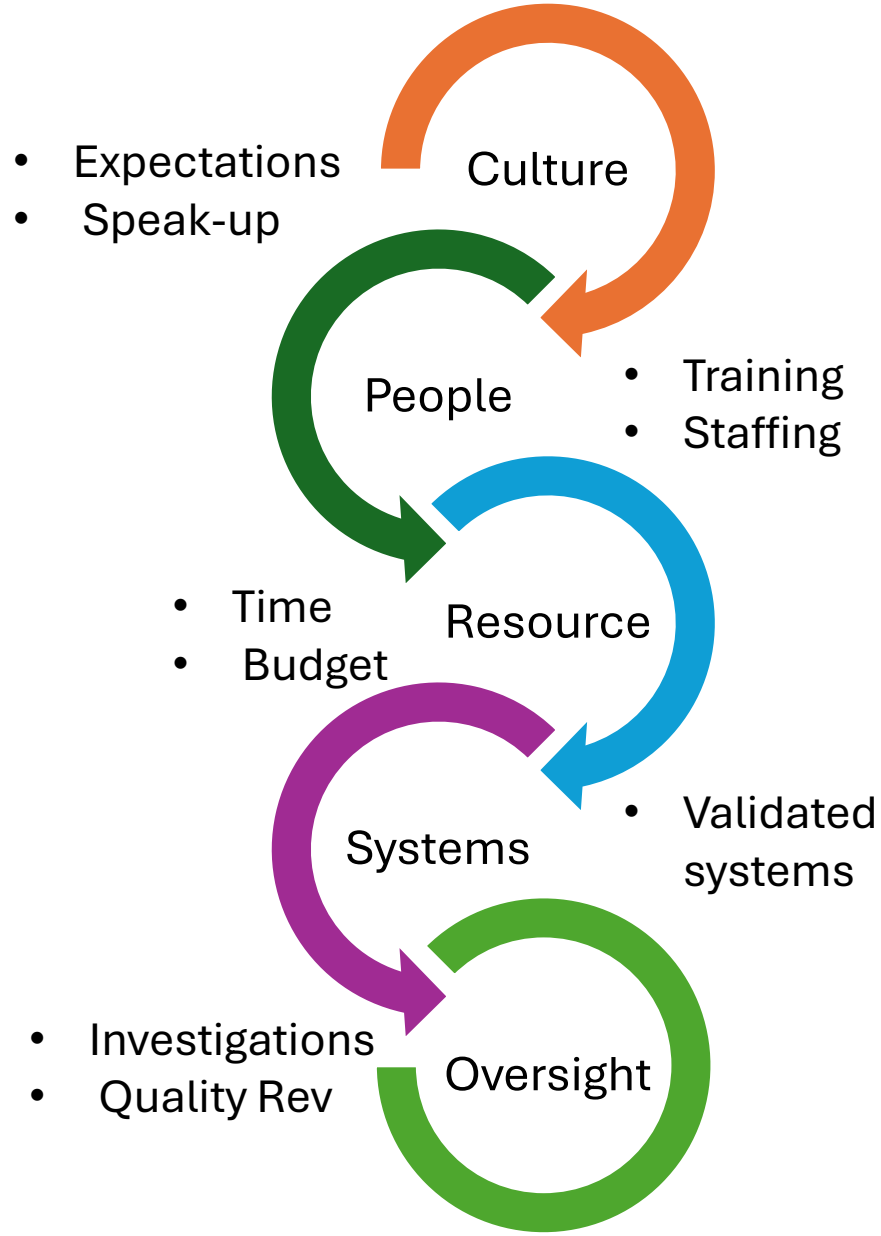
“Data Integrity starts before data is generated. It starts with management.”

Question:

"If management puts pressure on employees to achieve a desired result, can any computerized system alone guarantee Data Integrity?"



Management should provide:



"Management must create an environment where accurate data is more important than simply achieving a desired result."

The Pressure to “Get the Result”

Scenario

An analyst obtains:

Result = FAIL ❌

The production manager says: “We need the batch to pass. Please repeat the test.”

The analyst repeats the test.

Result = PASS ✅

What should happen?

A. Report only the passing result
B. Delete the first result
C. Preserve both results and investigate appropriately
D. Repeat until the result passes

management behavior can directly influence Data Integrity.

1. CULTURE



Management → Organization → People

What is Data Integrity Culture?

Data Integrity culture is the organizational environment in which people consistently understand, value, and protect the reliability of GxP data.

It is not just about having SOPs or validated computerized systems.

A strong culture means employees understand:

“Doing the right thing with data is part of my responsibility.”

“Data Integrity doesn't start with the HPLC, SCADA, LIMS, or ERP system. It starts with the organization's culture.”

Quality Culture vs Data Integrity Culture

Weak Culture	Strong Culture
“Don't make mistakes.”	“Report mistakes.”
Focus on passing results	Focus on reliable results
Blame individuals	Understand systems and behavior
Deviations are uncomfortable	Deviations are opportunities to learn
Data is viewed as paperwork	Data is viewed as evidence

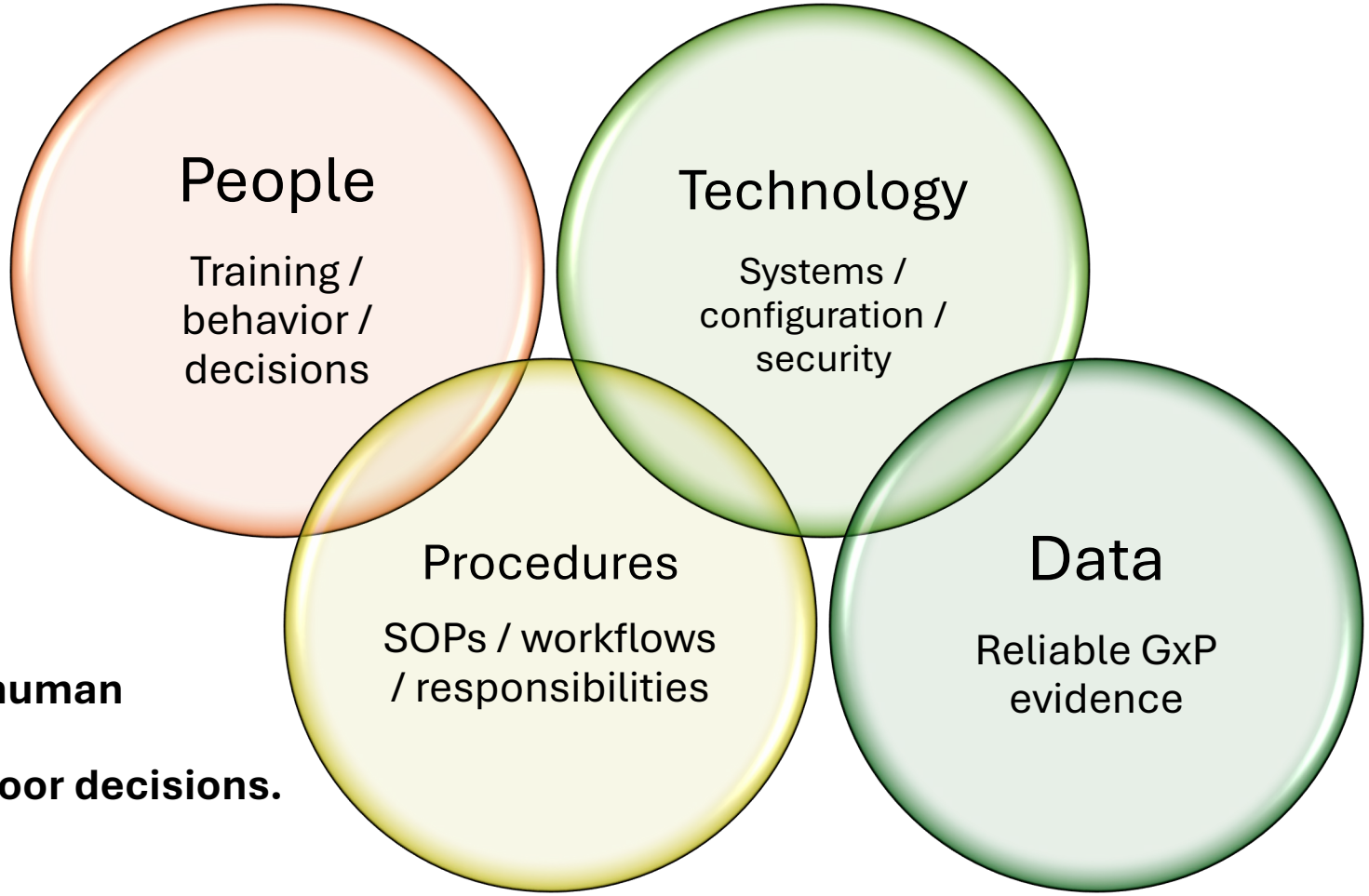
A strong Data Integrity culture does not mean “no mistakes.” It means mistakes are identified, reported, investigated and learned from.

SIVAND SANAT

People Are Part of the Control System

Think of the organization as a system:

DATA INTEGRITY CONTROL MODEL



Therefore:

Data Integrity is both a technical and human responsibility.

A validated system cannot compensate for poor decisions.

Speaking Up

A mature Data Integrity culture allows employees to say:

“I made a mistake.”

“This result doesn't look right.”

“I forgot to record the value at the time.”

“The system allowed me to change this data.”

without fear of inappropriate retaliation.

The organization should then ask:

“Why did the system/process allow this to happen?”

rather than immediately asking:

“Who is guilty?”

What Data Integrity is NOT

DATA INTEGRITY IS NOT:

- ❌ Only ALCOA+
- ❌ Only IT security
- ❌ Only validated software
- ❌ Only audit trails
- ❌ Only QA responsibility
- ❌ Only an SOP

Then:

DATA INTEGRITY IS:
People + Processes + Technology + Data Governance

2. PRINCIPLES

Data Integrity → Raw Data → Metadata → ALCOA+

Data Integrity is the extent to which data are complete, consistent, accurate, trustworthy and reliable, and are maintained throughout the data lifecycle.

Raw Data: The original record that represents the first capture of information, whether recorded on paper or electronically.

Metadata: Is information that describes the attributes of data and provides the context and meaning necessary to understand the data.

Metadata could tell us:

- **What?** Temperature
- **Where?** Cleanroom CR-101
- **When?** 29-Aug-2026, 14:05
- **Who/Source?** Temperature transmitter TT-101 / SCADA
- **Unit?** °C
- **Instrument?** TT-101
- **Status?** Normal
- **Method/system?** HVAC SCADA

Data* + *Metadata* = *Context & Meaning

Raw data
22.5°C
Metadata
TT-101 / CR-101 / 14:05 / °C / SCADA-01
Audit trail
User01 changed setpoint from 22°C → 23°C at 14:10

Metadata is not simply “extra information.”
“Without appropriate metadata, data may lose its context, meaning and ability to be fully understood.”

What is ALCOA+?

ALCOA consists of five fundamental characteristics:

A	Attributable	Who performed the activity?
L	Legible	Can the record be read and understood?
C	Contemporaneous	Was it recorded at the time?
O	Original	Is it the original record or a verified true copy?
A	Accurate	Does it correctly represent what happened?

The **“+”** extends this with:

Principle	Simple Meaning
Complete	Nothing relevant is missing
Consistent	Data follows the expected sequence and chronology
Enduring	The record remains preserved throughout retention
Available	It can be accessed when required

For example:

Principle	Pharmaceutical example
Attributable	Operator login identifies who performed the activity
Legible	Record remains readable throughout retention
Contemporaneous	Temperature recorded at the time of measurement
Original	Original electronic record retained
Accurate	Instrument value correctly recorded
Complete	All required results retained
Consistent	Chronology makes sense
Enduring	Record remains protected
Available	Data can be retrieved during inspection

3. CONTROLS



Control ≠ restriction only.

Control element	Purpose
1. Procedures	Define how data must be created, handled, reviewed, corrected, retained, and managed
2. Systems	Provide technical mechanisms to generate, process, store, and protect data
3. Audit Trail	Provides a history of who did what, when, and what changed
4. Access Control	Ensures only authorized users can perform permitted activities
5. Validation	Provides documented evidence that the system consistently performs as intended
6. Monitoring	Ensures controls continue to work and identifies deviations, unusual activity, or weaknesses

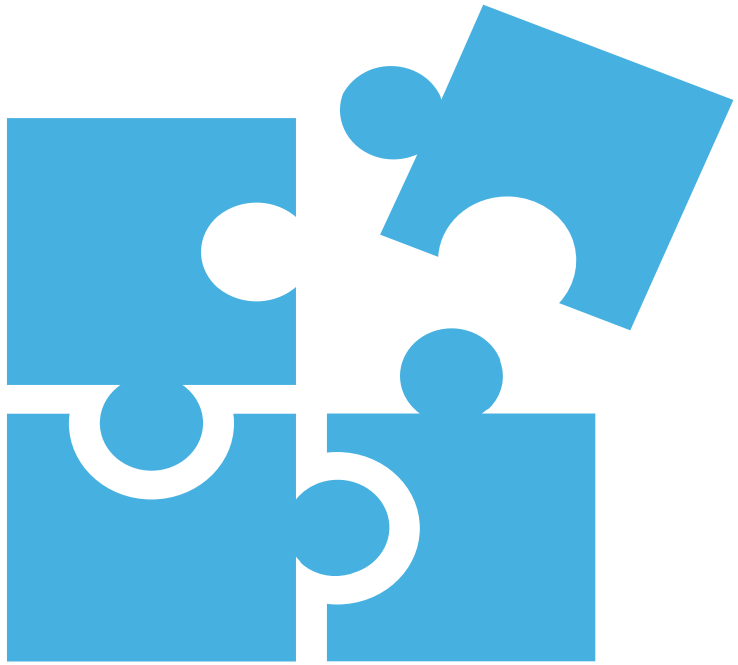
Data Integrity is not achieved by one control. It requires a system of interconnected controls.

4. Data Life Cycle



DATA INTEGRITY MUST BE MAINTAINED THROUGHOUT THE ENTIRE LIFECYCLE.

5. From Where to Start?/ How To Start?



WHERE TO START? — HOW TO START?

1. **GAP ANALYSIS**

   Where are we now? Current State → Expected State Gap

Current: Shared user account in SCADA

Expected: Unique user identification

Gap: Lack of individual accountability

2. IMPACT ASSESSMENT

What could be affected?

- 🧪 **GxP Data**
- 💊 **Product Quality**
- 👤 **Patient Safety**
- 📋 **Batch Release**
- ⚖️ **Regulatory Compliance**
- 🔍 **Data Traceability**
- 💰 **Business / Operations**

Not every data-integrity gap has the same impact.

3. HIGH-LEVEL RISK ASSESSMENT

How significant is the risk?

Risk = Impact × Likelihood

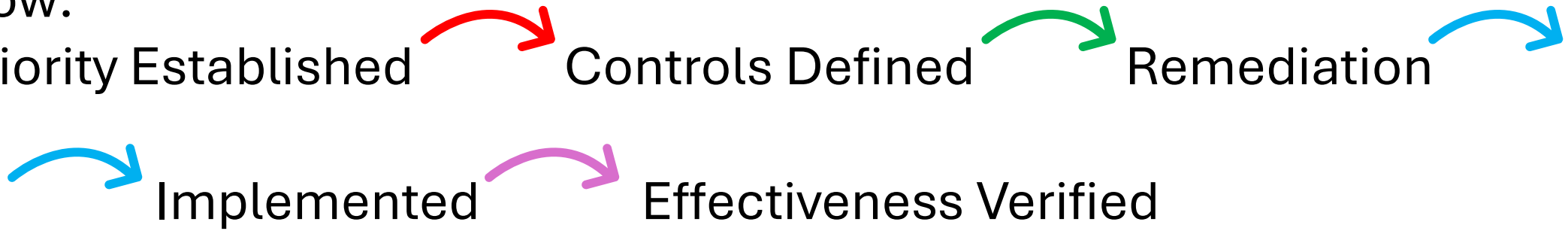
Risk	Priority	Typical response
🔴 High	Immediate	Remediation / CAPA
🟠 Medium	Planned	Risk-based improvement
🟢 Low	Monitor	Justification / monitoring

FMEA Technique= Severity x Occurrence x Detection= RPN

4. From Risk to Action

What should we address first?

Now:



6. References

- MHRA- “‘GxP’ Data Integrity Guidance and Definitions” March 2018.
- PIC/S- “GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS” July 2021.
- EU GMP Annex 11- “Computerized Systems” where applicable.
- ISPE- GAMP 5, where applicable.
- 21 CFR Part 11- “Electronic Records; Electronic Signatures” where applicable.

Thank you for your attention



Questions?

Contact Information: 09141009045
Email: qa@sivandsanat.com
LinkedIn: linkedin.com/in/hamed-benam-b6b42741

Appendix:

PHARMACEUTICAL DATA ECOSYSTEM

Raw materials
↓
Warehouse / ERP
↓
Manufacturing
↓
PLC / SCADA
↓
EMS / BMS
↓
Laboratory / HPLC
↓
LIMS
↓
QA Review
↓
Batch Release
↓
Archiving