PDA®

Parenteral Drug Association

Ireland Chapter

Data Integrity

Tuesday, 12th May 2015
The Hilton Hotel, Charlemont Place, Dublin 2

Data Integrity Seminar

Introduction

Commissioning Agents International

12 May 2014

Welcome and Agenda

Time	Topic	Speakers
08:30 – 09:00	REGISTRATION	
09:00 – 09:15	Introduction	Alice Redmond/Brendan Walsh, CAI
09:15 – 10:00	Data Integrity: A perspective from the medical device regulatory and standards framework	Paul Scannel, NSAI
10:00 – 10:45	Data Integrity: A Regulator’s Perspective	Ciara Turley, HPRA
10:45 – 11:15	BREAK	
11:15 – 12:00	Data Integrity: an Industry perspective	Brian O’Broin, VALIDANT
12:00 – 12:45	Data Integrity Governance Planning	Ursula Greene, McGee Pharma
12:45 – 13:45	LUNCH	
13:45 – 14:30	Data Integrity: A Practical Approach for the QC Laboratory	Dan Latham-Timmons, Amgen
14:30 – 15:30	Focus on Patient and Product Quality as the foundation for Data Integrity	Madlene Dole, Novartis
15:30 – 16:00	BREAK	
16:00 – 16:30	DI – the reality	Brendan Walsh, Novartis – Alcon Division
16:30 – 17:00	Q&A discussion with all presenters	

PDA®
Parenteral Drug Association
Ireland Chapter

Definition – Lets set the scene

Data integrity is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. Data integrity is imposed within a system at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines.

Data integrity – Why a hot topics now ?

- Agencies expects that pharmaceutical companies should retain complete and accurate records and all raw data and to make that available to inspectors
- The integrity of data generated by a regulated pharmaceutical companies and laboratories matters most, because properly recorded information is the basis for manufacturers to assure product identity, strength, purity, and safety and non-compliances found in the integrity of data leads warning letters and a regulatory action from the agencies

PDA® Parenteral Drug Association Ireland Chapter

Regulatory Basis- Key docs

- **MHRA GMP Data Integrity Definitions and Guidance for Industry ---**Published March 2015
- FDA's Application Integrity Policy at www.fda.gov
- Eudralex-Volume 4 Good manufacturing practice (GMP) Guidelines

PDA® Parenteral Drug Association Ireland Chapter

Warning letters issued by FDA in year 2014-15

- Micro Labs Limited 1/9/15
- Apotex Research Private Limited 1/30/15
- Cadila Pharmaceuticals Limited 10/15/14
- Apotex Pharmachem India Pvt Ltd. 6/16/14
- Tianjin Zhongan Pharmaceutical Co., Ltd. 6/10/14
- Sun Pharmaceutical Industries Limited – Karkhadi 5/7/14
- Canton Laboratories Pvt. Ltd. 2/27/14
- Usv Limited 2/6/14

PDA®
Parenteral Drug Association
Ireland
Chapter

Challenges noted by the agencies---

- **Non contemporaneous Recording:** Failure to record activities at the time when activity was performed. There is evidence that the records were signed by company personnel when the person was actually absent on that day.
- **Document back-dating:** Backdating stability test results to meet the required commitments.
- **Copy of existing data as new information:** Test results from previous batches were used to substitute testing for another batch or acceptable test results were created without performing the test.
- **Re-running samples to obtain better results:** Multiple analyses of assay were done with the same sample without adequate justification and in some cases samples were tested unofficially or as a trial analysis until desired test results obtained.
- **Data fabrication and data discarding:** Original raw data and records were altered for e.g., by using of correction fluid or Manipulation of a poorly defined analytical procedure and associated data analysis in order to obtain passing results.

Agenda

Time	Topic	Speakers
08:30 – 09:00	REGISTRATION	
09:00 – 09:15	Introduction	Alice Redmond/Brendan Walsh, CAI
09:15 – 10:00	Data Integrity: A perspective from the medical device regulatory and standards framework	Paul Scannel, NSAI
10:00 – 10:45	Data Integrity: A Regulator’s Perspective	Ciara Turley, HPRA
10:45 – 11:15	BREAK	
11:15 – 12:00	Data Integrity: an Industry perspective	Brian O’Broin, VALIDANT
12:00 – 12:45	Data Integrity Governance Planning	Ursula Greene, McGee Pharma
12:45 – 13:45	LUNCH	
13:45 – 14:30	Data Integrity: A Practical Approach for the QC Laboratory	Dan Latham-Timmons, Amgen
14:30 – 15:30	Focus on Patient and Product Quality as the foundation for Data Integrity	Madlene Dole, Novartis
15:30 – 16:00	BREAK	
16:00 – 16:30	DI – the reality	Brendan Walsh, Novartis – Alcon Division
16:30 – 17:00	Q&A discussion with all presenters	

PDA®
Parenteral Drug Association
Ireland Chapter

NSAI
Certification

Data Integrity:

A Perspective from the Medical Device Regulatory and Standards Framework

PDA Ireland Chapter
May 12th 2015

Paul Scannell MSc PhD
Senior Scientific Officer
NSAI

“Data integrity is a prerequisite for the regulated healthcare industry as decisions and assumptions on product quality and compliance with the applicable regulatory requirements are made based on data”

Institute of Validation Technology

NSAI Certification

Agenda →

Agenda

PART I

- European Regulations, Directives & Standards Intro
- Regulatory Framework & Data Integrity
  - Current Framework
  - Proposed Framework

PART II

- Standards & Data Integrity
  - Product Assessment
  - QMS Assessment

Part I→

PART I

EU Regs. & Dir.→

European Regulations & Directives

Regulations, Directives & Standards

Regulation

A "regulation" is a binding legislative act. It must be applied in its entirety across the EU.

Directive

A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how *i.e.* Directives are transposed into National law.

Harmonised Standards

European standard (EN) adopted on the basis of a mandate by the Commission and published in the Official Journal of the EU. Presumption of conformity to EU legislation when used.

Current EU Regs. & Dir.→

Current MD Regulatory Framework

Three primary European medical device Directives and related Statutory Instruments (European Directives are transposed into National law).

Device	Directive	Statutory Instrument
General Medical Devices	93/42/EEC	S.I. No. 252 of 1994
In Vitro Diagnostic Medical Devices	98/79/EEC	S.I. No. 304 of 2001
Active Implantable Medical Devices	90/385/EEC	S.I. No. 253 of 1994

Several modifying/implementing Directives/Regulations:

I. 2010/227/EU - EUDAMED
II. 2007/47/EC – Revision to MDD and AIMD
III. 2005/50/EC – Reclassification of joint replacements
IV. 2003/32/EC – Tissues of animal origin
V. 2003/12/EC – Reclassification of breast implants
VI. 2000/70/EC – Devices incorporating blood derivatives
VII. EU No. 920/2013 - Designation and the supervision of notified bodies

Proposed EU Regs.→

Proposed MD Regulatory Framework

Device	Directive	Statutory Instrument
General Medical Devices	93/42/EEC	S.I. No. 252 of 1994
In Vitro Diagnostic Medical Devices	98/79/EEC	S.I. No. 304 of 2001
Active Implantable Medical Devices	90/385/EEC	S.I. No. 253 of 1994

Device	Regulation
General Medical Devices + Active Implantable Medical Devices	**A proposal for a Regulation on medical devices** (to replace: Directive 90/385/EEC regarding active implantable medical devices and Directive 93/42/EEC regarding medical devices)
In Vitro Diagnostic Medical Devices	**A proposal for a Regulation on *in vitro* diagnostic medical devices** (to replace Directive 98/79/EC regarding in vitro diagnostic medical devices).

Proposed EU Regs.→

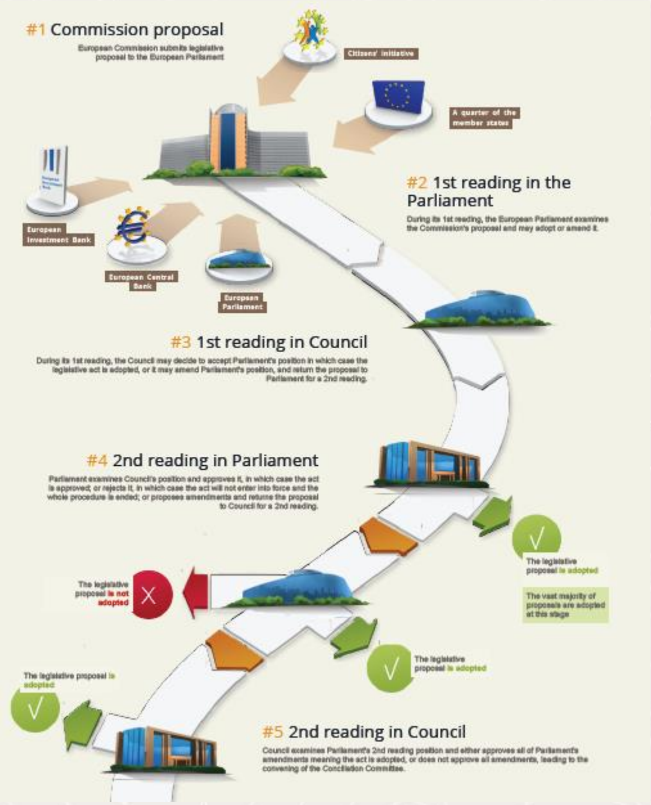
Proposed MD Regulatory Framework

Device	Directive	Statutory Instrument
General Medical Devices	93/42/EEC	S.I. No. 252 of 1994
In Vitro Diagnostic Medical Devices	98/79/EEC	S.I. No. 304 of 2001
Active Implantable Medical Devices	90/385/EEC	S.I. No. 253 of 1994

EU Leg. Procedure →

Origins of Regulations & Directives

The Ordinary Legislative Procedure


Citizens' initiative
A quarter of the member states
European Investment Bank
European Central Bank
European Parliament
The legislative proposal is adopted
The vast majority of proposals are adopted at this stage
The legislative proposal is not adopted
The legislative proposal is adopted
The legislative proposal is adopted

#1 Commission proposal

European Commission submits legislative proposal to the European Parliament

#2 1st reading in the Parliament

During its 1st reading, the European Parliament examines the Commission's proposal and may adopt or amend it.

#3 1st reading in Council

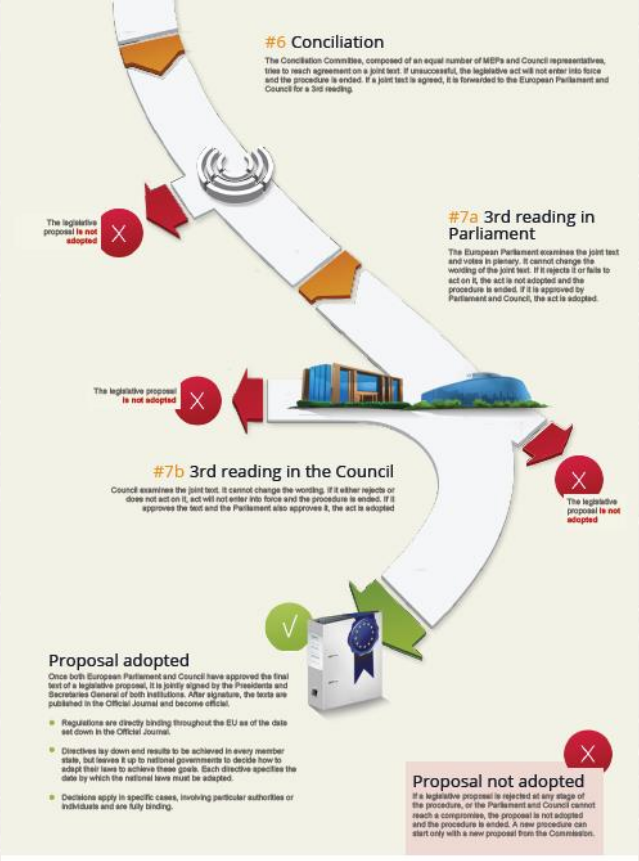
During its 1st reading, the Council may decide to accept Parliament's position in which case the legislative act is adopted, or it may amend Parliament's position, and return the proposal to Parliament for a 2nd reading.

#4 2nd reading in Parliament

Parliament examines Council's position and approves it, in which case the act is approved; or rejects it, in which case the act will not enter into force and the whole procedure is ended; or proposes amendments and returns the proposal to Council for a 2nd reading.

#5 2nd reading in Council

Council examines Parliament's 2nd reading position and either approves all of Parliament's amendments meaning the act is adopted, or does not approve all amendments, leading to the convening of the Conciliation Committee.


The legislative proposal is not adopted
The legislative proposal is not adopted
The legislative proposal is not adopted

#6 Conciliation

The Conciliation Committee, composed of an equal number of MEPs and Council representatives, tries to reach agreement on a joint text. If unsuccessful, the legislative act will not enter into force and the procedure is ended. If a joint text is agreed, it is forwarded to the European Parliament and Council for a 3rd reading.

#7a 3rd reading in Parliament

The European Parliament examines the joint text and votes in plenary. It cannot change the wording of the joint text. If it rejects it or fails to act on it, the act is not adopted and the procedure is ended. If it is approved by Parliament and Council, the act is adopted.

#7b 3rd reading in the Council

Council examines the joint text. It cannot change the wording. If it either rejects or does not act on it, act will not enter into force and the procedure is ended. If it approves the text and the Parliament also approves it, the act is adopted

Proposal adopted

Once both European Parliament and Council have approved the final text of a legislative proposal, it is jointly signed by the Presidents and Secretaries General of both institutions. After signature, the texts are published in the Official Journal and become official.

- Regulations are directly binding throughout the EU as of the date set down in the Official Journal.
- Directives lay down end results to be achieved in every member state, but leaves it up to national governments to decide how to adapt their laws to achieve these goals. Each directive specifies the date by which the national laws must be adapted.
- Decisions apply in specific cases, involving particular authorities or individuals and are fully binding.

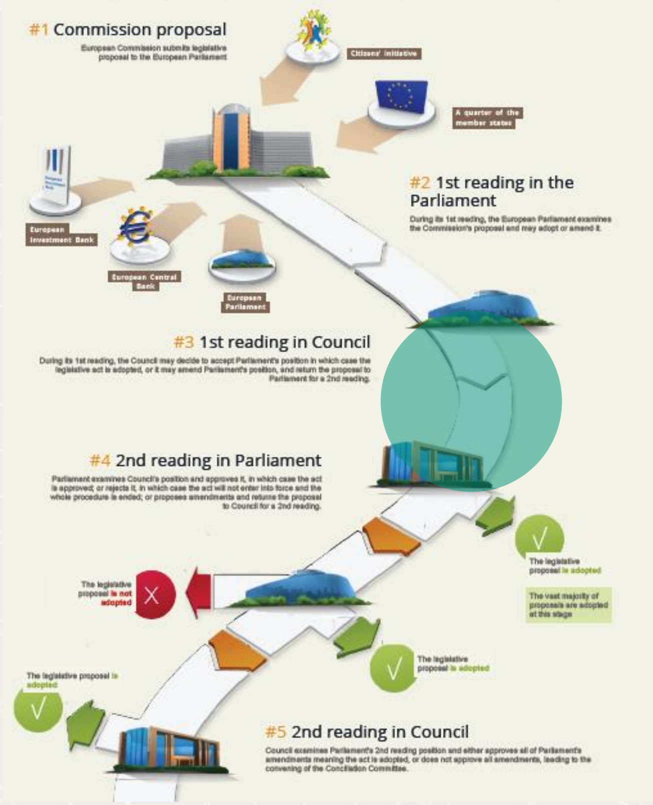
Proposal not adopted

If a legislative proposal is rejected at any stage of the procedure, or the Parliament and Council cannot reach a compromise, the proposal is not adopted and the procedure is ended. A new procedure can start only with a new proposal from the Commission.

EU Leg. Procedure (now) →

Origins of Regulations & Directives

The Ordinary Legislative Procedure



#1 Commission proposal

European Commission submits legislative proposal to the European Parliament

#2 1st reading in the Parliament

During its 1st reading, the European Parliament examines the Commission's proposal and may adopt or amend it.

#3 1st reading in Council

During its 1st reading, the Council may decide to accept Parliament's position in which case the legislative act is adopted, or it may amend Parliament's position, and return the proposal to Parliament for a 2nd reading.

#4 2nd reading in Parliament

Parliament examines Council's position and approves it, in which case the act is approved; or rejects it, in which case the act will not enter into force and the whole procedure is ended; or proposes amendments and returns the proposal to Council for a 2nd reading.

#5 2nd reading in Council

Council examines Parliament's 2nd reading position and either approves all of Parliament's amendments meaning the act is adopted, or does not approve all amendments, leading to the convening of the Conciliation Committee.

Citizens' initiative
A quarter of the member states
European Investment Bank
European Central Bank
European Parliament
The legislative proposal is adopted
The vast majority of proposals are adopted at this stage
The legislative proposal is not adopted
The legislative proposal is adopted
The legislative proposal is adopted

Unlikely to be adopted in 2015 under the current presidency of Council of the European Union (Latvia).

Potentially during Luxembourg's presidency.

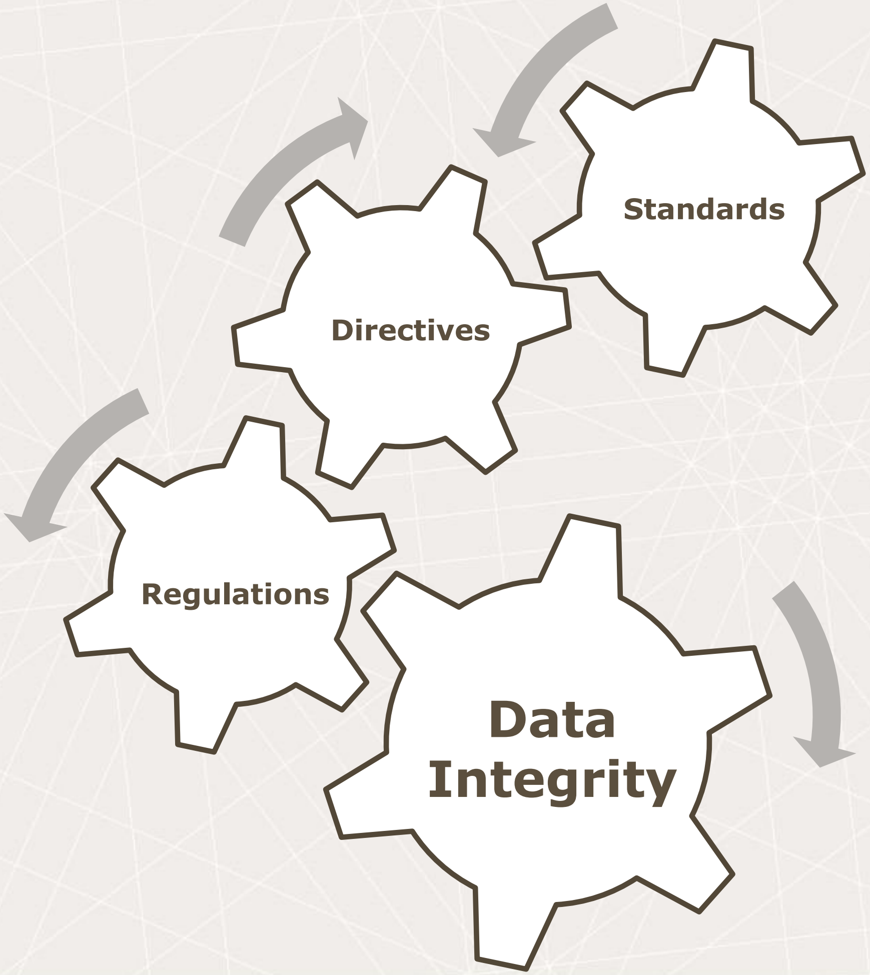
Key topics:

- High Risk Devices
- Re-processing
- Scrutiny procedure and notified bodies
- Ingestible and aesthetic devices

Updates and summaries on status:
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0266%28COD%29

Regs + Data Integrity→

Regulatory Framework & Data Integrity



Count Current v Proposed →

Regulatory Framework & Data Integrity

Current Medical Device Directives V Proposed Regulations

Illustrative word count

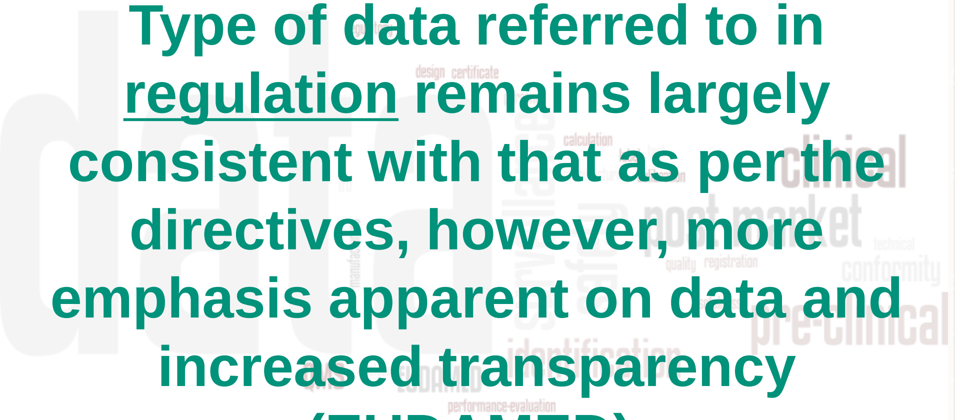
Current Directives			
	Data Integrity	Integrity	Data
MDD	0	1	51
AIMD	0	1	39
IVDD	0	3	39

Proposed Regulations			
	Data Integrity	Integrity	Data
MDR	0	6	140
IVDR	0	6	91

Integrity:

- professional integrity of notified bodies
- packaging & device integrity
- integrity of patients / the person

Data:

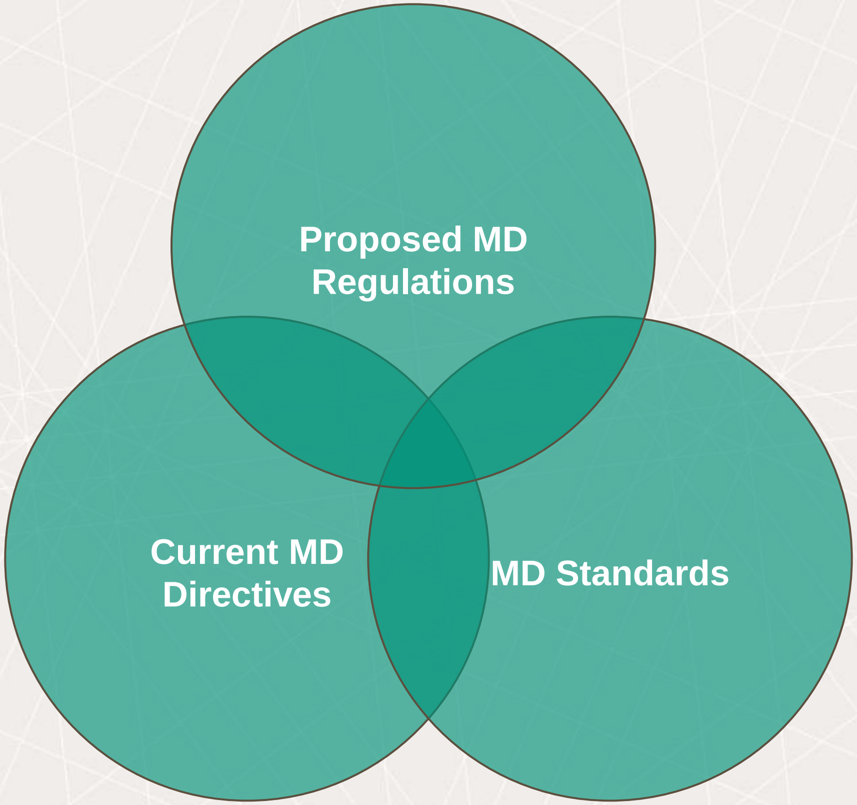


Type of data referred to in regulation remains largely consistent with that as per the directives, however, more emphasis apparent on data and increased transparency (EUDAMED).

Data Integrity is implicit not explicit

Intro Proposed →

Regulatory Framework & Data Integrity

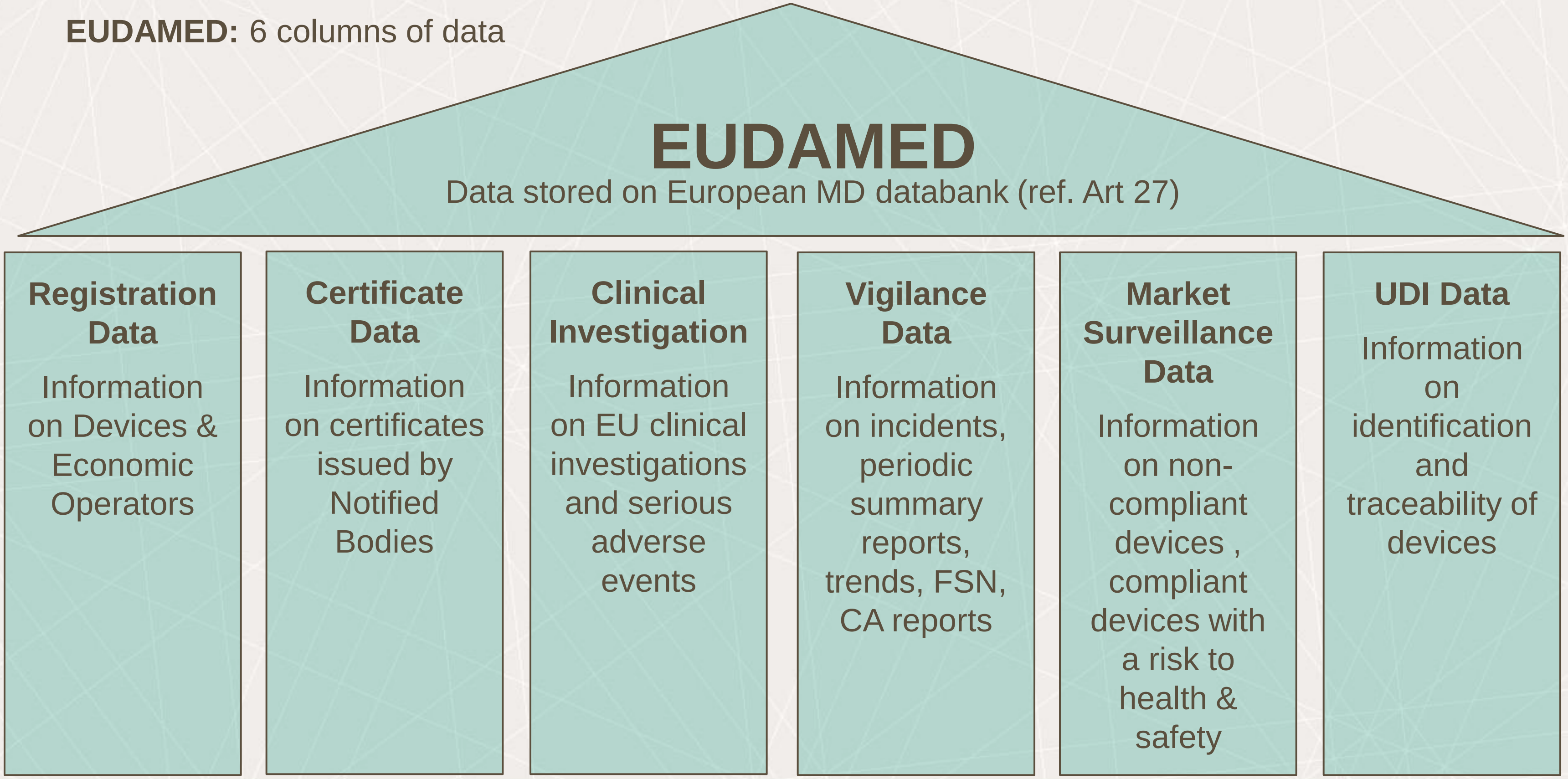


Proposed EUDAMED →

Regulatory Framework & Data Integrity

Proposed Medical Device Regulations

EUDAMED: 6 columns of data



EUDAMED

Data stored on European MD databank (ref. Art 27)

Registration Data
Information on Devices & Economic Operators

Certificate Data
Information on certificates issued by Notified Bodies

Clinical Investigation
Information on EU clinical investigations and serious adverse events

Vigilance Data
Information on incidents, periodic summary reports, trends, FSN, CA reports

Market Surveillance Data
Information on non-compliant devices , compliant devices with a risk to health & safety

UDI Data
Information on identification and traceability of devices

Proposed EUDAMED contd. →

Regulatory Framework & Data Integrity

Proposed Medical Device Regulations

EUDAMED:

All the information collated and processed by EUDAMED shall be accessible to the Member States and to the Commission.

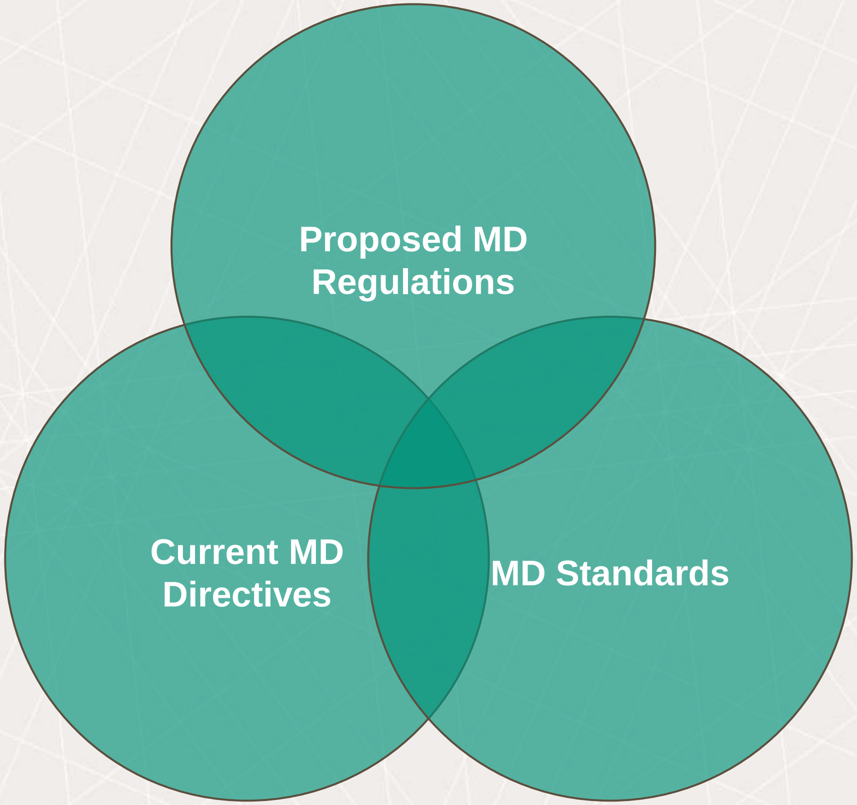
Certain information will be made available to Notified Bodies.

A large part of the information in EUDAMED will become publicly available.

Additionally:

Manufacturers of high-risk devices to make **publicly available** a summary of safety and performance with key elements of the supporting **clinical data.**

Regulatory Framework & Data Integrity



Imp. Reg. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?

Imp. Reg. contd. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?

Recital (4)

Designation [of notified bodies] should be assessed by teams of assessors representing the knowledge and experience of different Member States and of the Commission. To facilitate such assessments, certain essential documents should be accessible to those involved in these activities

Imp. Reg. contd. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?

Article 3.2

Representatives of designating authorities of two other Member States shall, in coordination with the designating authority of the Member State in which the conformity assessment body is established and together with a representative of the Commission, participate to the assessment of the conformity assessment body

Imp. Reg. contd. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?

Article 5.1

the designating authority of the Member State where the notified body is established shall assess an appropriate number of notified body's reviews of the manufacturer's clinical evaluations and shall carry out an appropriate number of file reviews, surveillance on-site assessments

Imp. Reg. contd. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?

DA / CA

NB

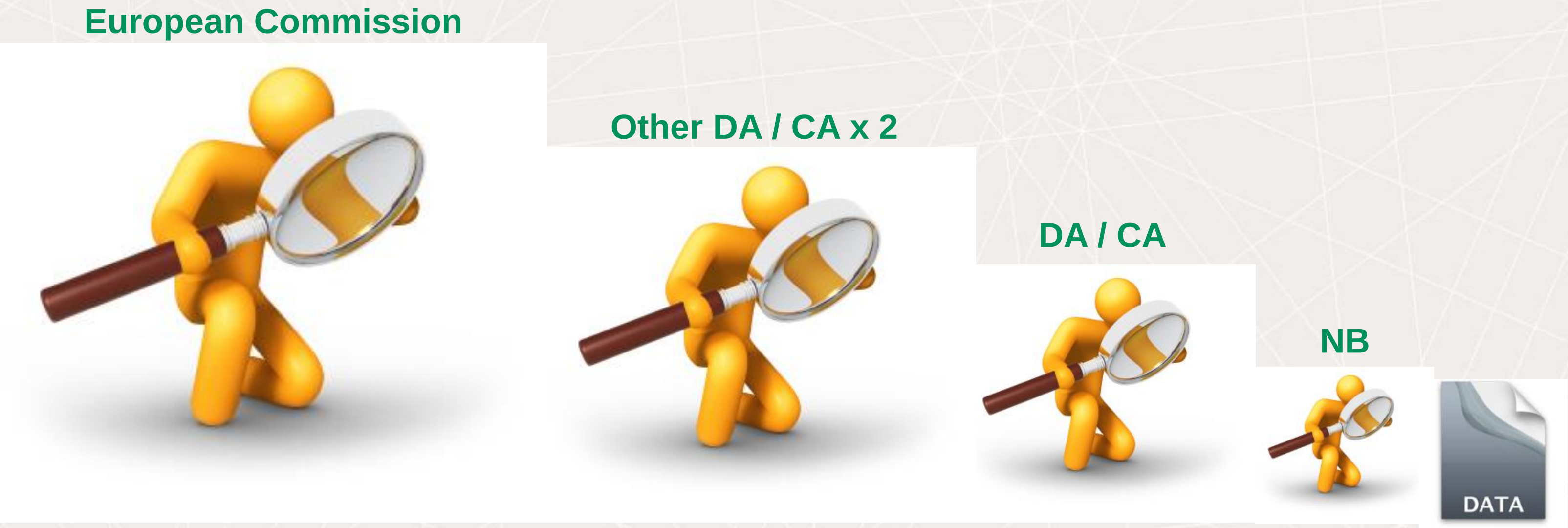
Imp. Reg. contd. →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards

Commission Implementing Regulation (EU) No 920/2013

- Designation and supervision of Notified Bodies
- Implications for manufacturers and data integrity?



European Commission

Other DA / CA x 2

DA / CA

NB

EC. Rec. (prod) →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards
Commission Recommendation 2013/473/EU

- Concerns audits and assessments performed by notified bodies
- Implications for manufacturers and data integrity?

Product Assessment (Annex I)

Notified bodies should …

Verify all documentation related to the device’s conformity assessment.

Verify that the technical documentation is correct, consistent, relevant, up-to-date and complete.

Verify documentation can unequivocally be attributed to the device examined.

- Qualification & Classification
- Essential Requirements
- Risk Assessment
- Pre-clinical & Clinical
- Declaration of Conformity

EC. Rec. (QMS) →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards
Commission Recommendation 2013/473/EU

- Concerns audits and assessments performed by notified bodies
- Implications for manufacturers and data integrity?

Quality System Assessment (Annex II)

Notified Bodies should …

Verify product identification system and procedures relating to the product documentation covers all products intended to be placed on the market or put into service and are covered by the necessary certificates.

Verify that the manufacturer's procedures are up-to-date, complete, consistent and correct (classification, risk management, clinical evaluations, design & development, PMCF etc.)

Verify that the manufacturer controls the manufacturing environment and processes.

Verify the traceability of materials and components, from entry into the manufacturer's premises to the delivery of the final product

Verify that the documentation and records are up-to-date, consistent, complete, correct.

NSAI Certification

EC. Rec. (UAA) →

Regulatory Framework & Data Integrity

Current Medical Device Directives & Standards
Commission Recommendation 2013/473/EU

- Concerns audits and assessments performed by notified bodies
- Implications for manufacturers and data integrity?

Unannounced audits (Annex III)

Notified Bodies …

Should carry out unannounced audits at least once every third year. Higher frequency for high risk devices or devices subject to frequent non- conformities.

- includes the verification of the traceability of all critical components and materials and of the manufacturer's traceability system
- Should check in more detail at least two critical processes

May visit one of the premises of the manufacturer's critical subcontractors or crucial suppliers .

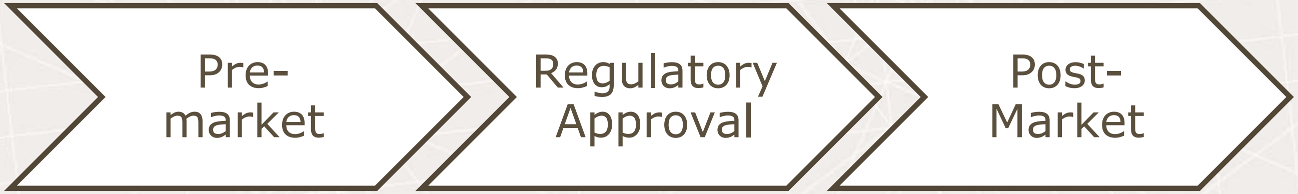
Part II →

PART II

Intro →

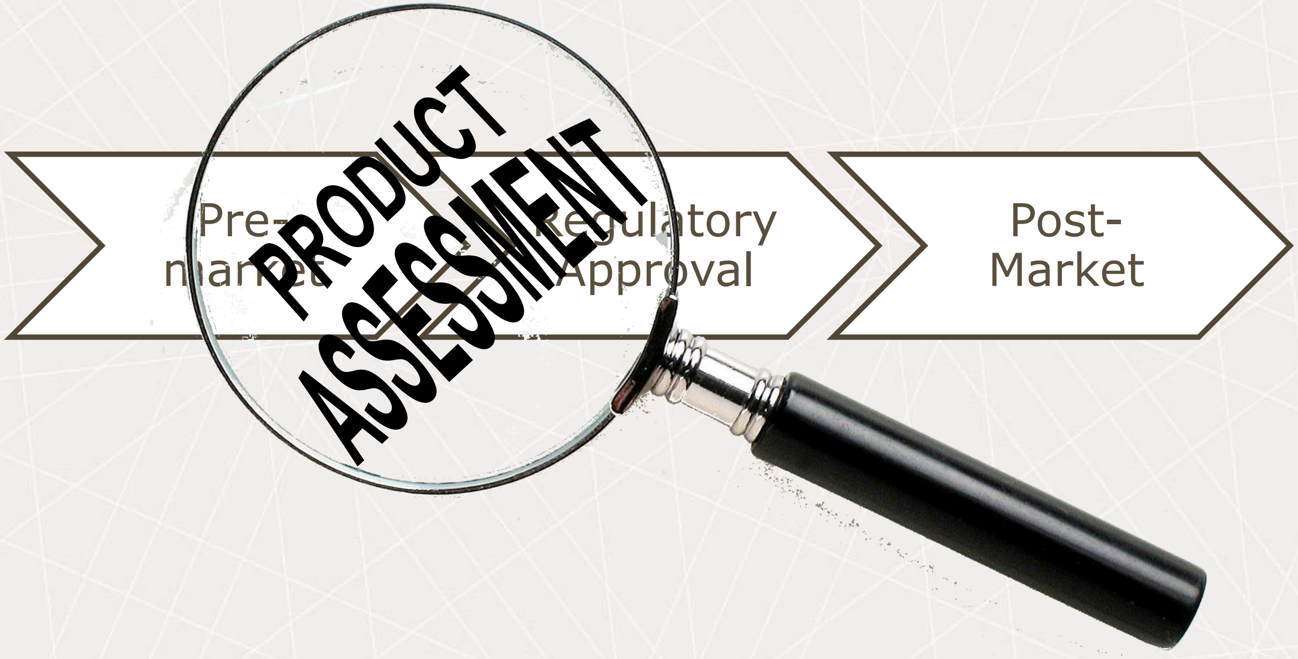
Standards & Data Integrity

Product Assessment



Standards & Data Integrity

Product Assessment



Pre-market

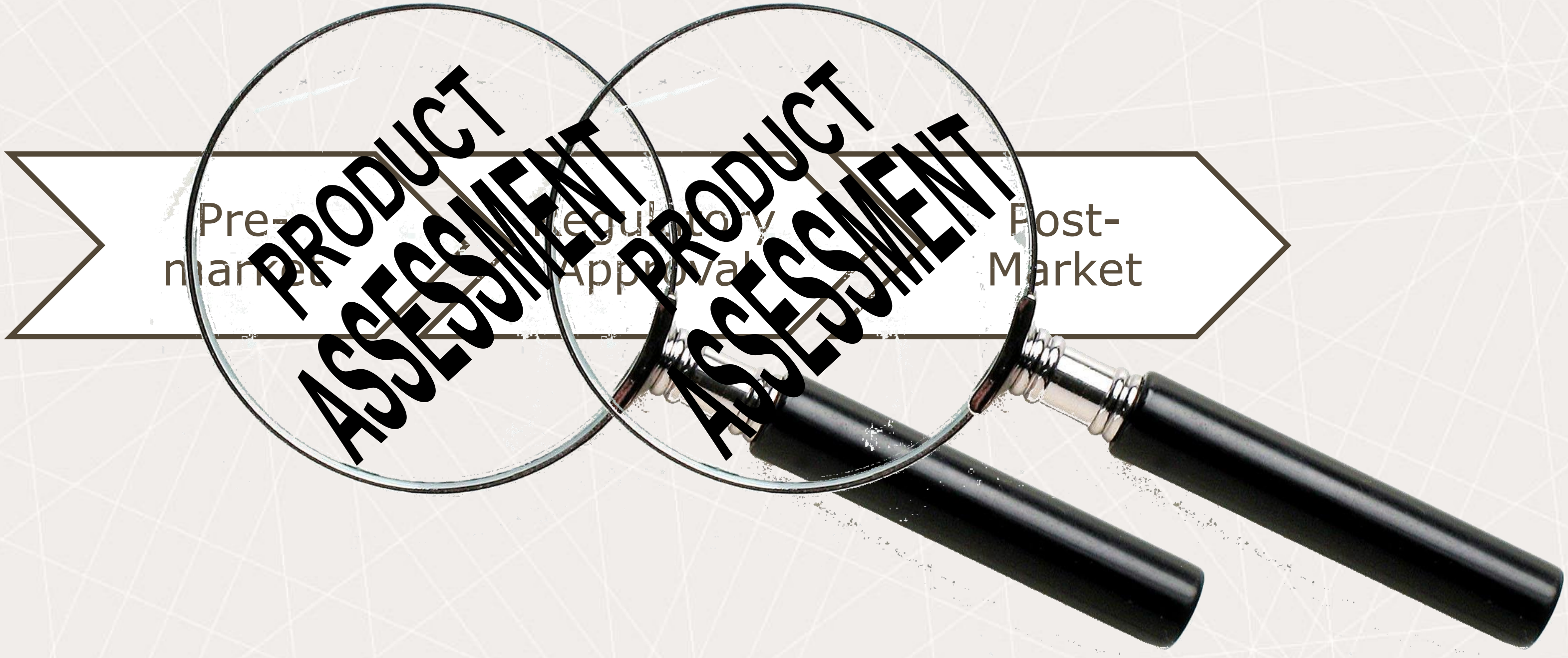
Regulatory Approval

Post-Market

Intro →

Standards & Data Integrity

Product Assessment



Prod. Assess.→

Standards & Data Integrity

Product Assessment

Device description
Device intended use
Device classification
Device labelling & IFU
Essential requirements compliance
Harmonised standards compliance
Complaint/vigilance evaluation
Risk Assessment
Pre-clinical testing
Stability
Biocompatibility & Sterilisation
Clinical evaluation

Data reviewed by NSAI

- New applications
- Substantial change requests
- Re-certification

Majority of data generated & compiled in line with relevant harmonised standards and reviewed against same.

NSAI Certification

Standards & Data Integrity

Product Assessment

EN ISO 14155 - Clinical investigation of medical devices for human subjects - Good clinical practice

§ 6.8 Document & Data Control

- Assurance of document and data control and traceability.
- Copies / printouts of original source document to be signed and dated by a member of the investigation site team with a statement that it is a true reproduction of the original source document.
- The data reported on the CRFs to be derived from source documents and be consistent with these source documents, and any discrepancies shall be explained in writing.
- CIP specifies what data can be recorded directly in the CRFs. The CRFs shall be signed and dated by the principal investigator or authorized designee(s). Any change/correction to data reported on a CRF shall be dated, initialled and explained if necessary, and shall not obscure the original entry (i.e. an audit trail shall be maintained); this applies to both written and electronic changes or corrections.

Prod. Assess. 14155 contd. →

Standards & Data Integrity

Product Assessment

EN ISO 14155 - Clinical investigation of medical devices for human subjects - Good clinical practice

§ 6.8 Document & Data Control

- Electronic clinical data systems must:
  - ensure accuracy of reports
  - maintain an audit/data/edit trail
  - prevent unauthorized access to the data
  - Maintain list of who accessed and dates of access
  - maintain adequate backup, retention and irretrievability of the data

Analysis of the all clinical data = clinical evaluation

Clinical Evaluation Report is a key document reviewed as part of the Medical Device CE marking process.

Prod. Assess. EN ISOs →

Standards & Data Integrity

Product Assessment

EN ISO 5840 - Cardiovascular implants - Cardiac Valve Prostheses

§ 7 Design verification testing and analysis/design validation

Verification testing to demonstrate that the device specifications result
meet the design specifications (design output meets design input).

The protocols shall identify the test purpose, set-up, equipment (specifications, calibration, etc.), test conditions, acceptance criteria and sample quantities tested.

EN ISO 11137 - Sterilization of health care products

§ 4.1 Documentation

Procedures for development, validation, routine control and product release from sterilization shall be specified.

Documents and records shall be reviewed and approved by designated personnel and controlled.

Prod. Assess. e.g.→

Standards & Data Integrity

Product Assessment

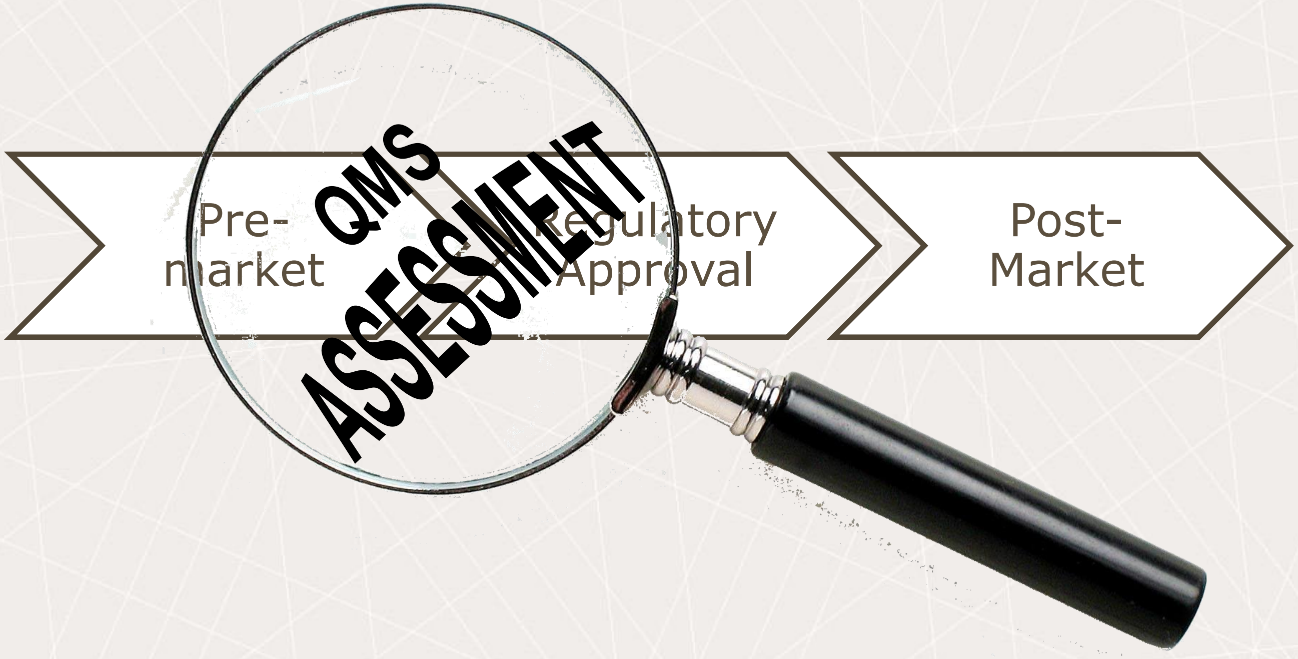
Examples of Data Integrity Issues experienced During Product Reviews

Undocumented Deviations:

- Product and/or test specs amended during verification and validation testing
- Out of spec result ignored
- Protocol sample size not adhered to and sample size justification
- Re-use of test specimens – validity of data generated
- Inconsistent protocol and test report rev number
- Test report summary inconsistent with raw data including altered results
- Testing duration cut short
- Reports not signed off at appropriate level or missing signatures
- Expertise of authors (biocomp and clinical)
- Scope of documentation not consistent with device models
- At recertification undeclared changes to specifications
- Tech file not kept up-to-date with regulatory environment (*e.g.* standards)

Standards & Data Integrity

Quality Management System Assessment

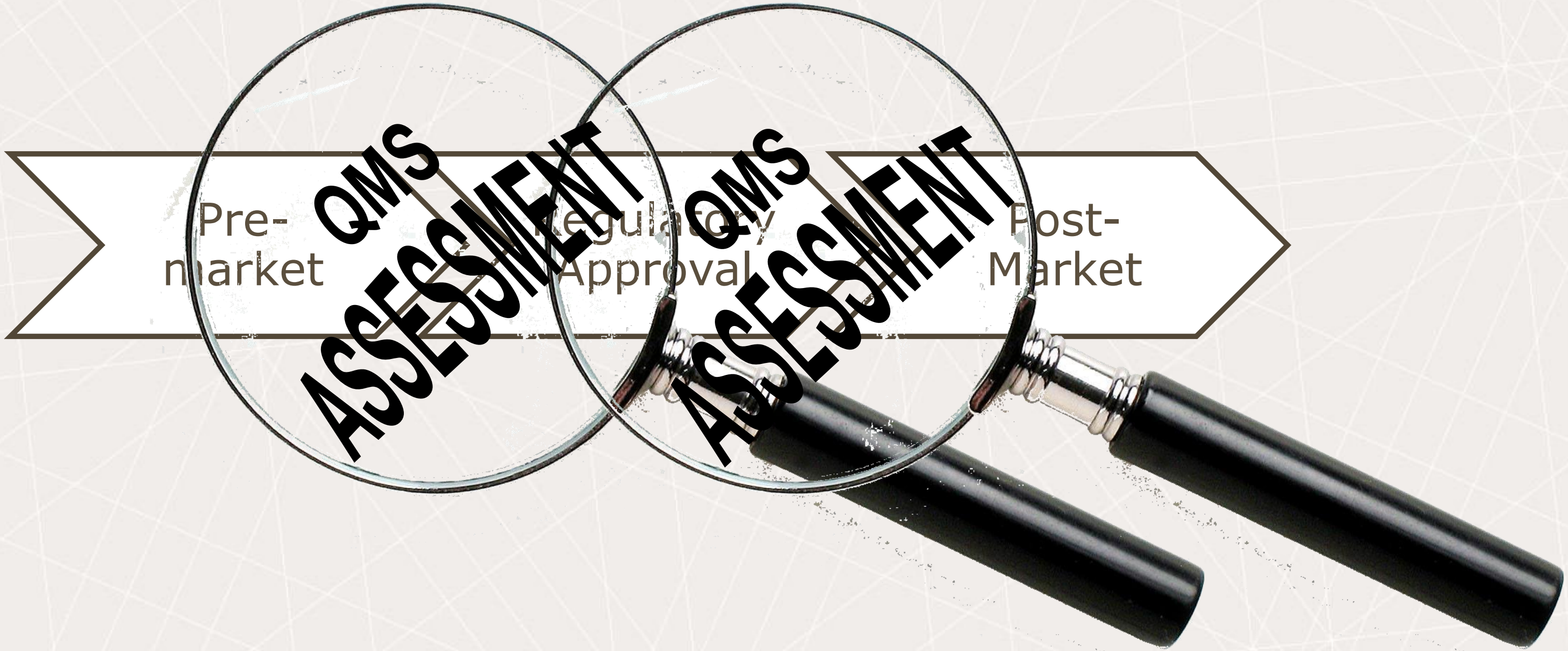


NSAI Certification

QMS. Assess. →

Standards & Data Integrity

Quality Management System Assessment



Standards & Data Integrity

Quality Management System Assessment

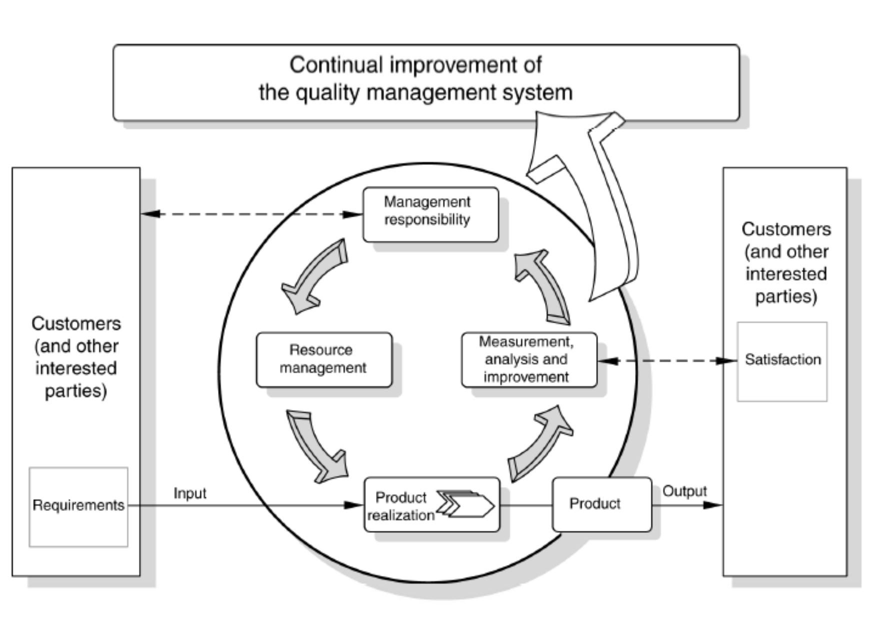
EN ISO 13485

Develop, implement and improve the effectiveness of a quality management system

Process approach
Plan-Do-Check-Act

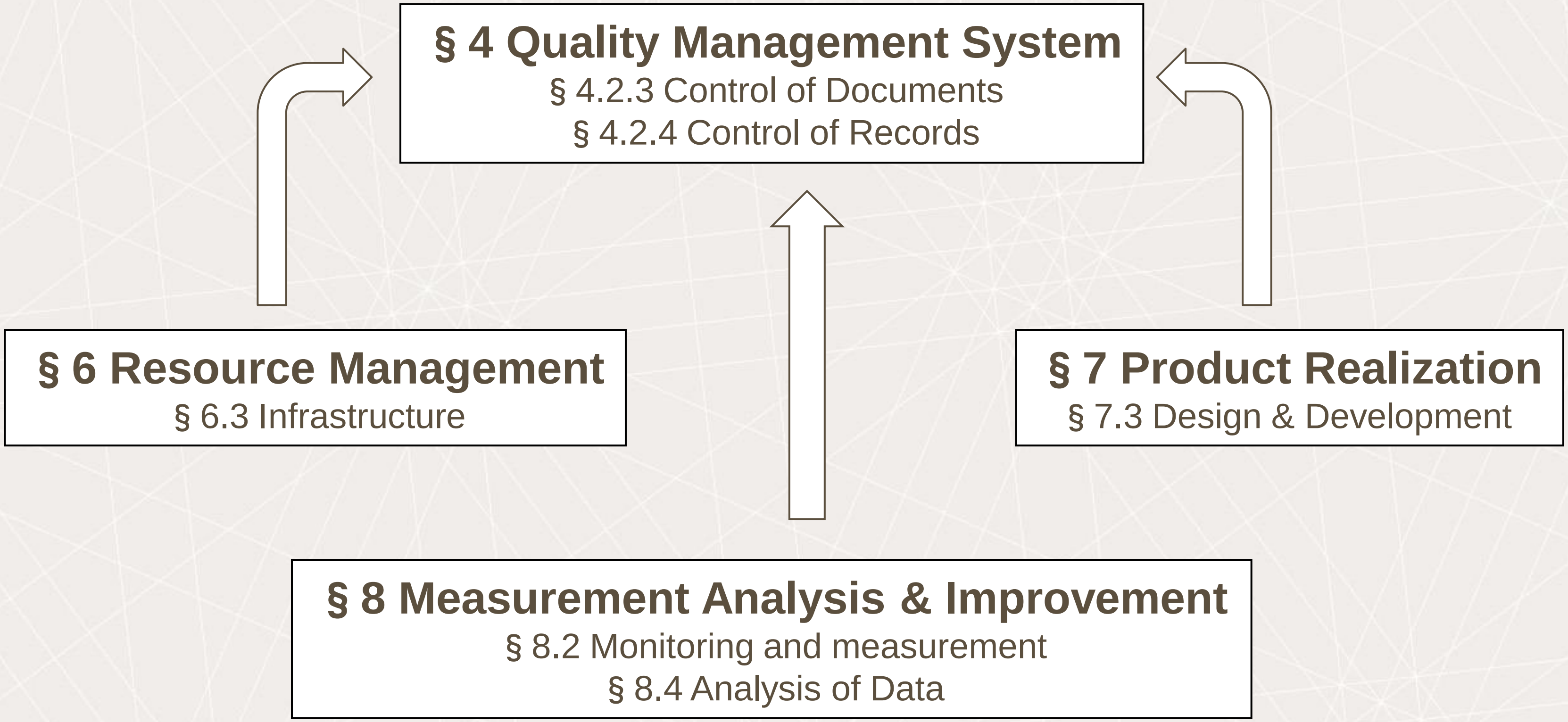
Output from one process can directly form the input to the next

§ **4** Quality Management System*
§ **5** Management Responsibility
§ **6** Resource Management*
§ **7** Product Realization*
§ **8** Measurement Analysis & Improvement*



Standards & Data Integrity

Quality Management System Assessment



§ 4 Quality Management System
§ 4.2.3 Control of Documents
§ 4.2.4 Control of Records

§ 6 Resource Management
§ 6.3 Infrastructure

§ 7 Product Realization
§ 7.3 Design & Development

§ 8 Measurement Analysis & Improvement
§ 8.2 Monitoring and measurement
§ 8.4 Analysis of Data

Note: Non-exhaustive Examples

§ 6.3 Infra. →

Standards & Data Integrity

Quality Management System Assessment

§ 6.3 Infrastructure

Determine, provide and maintain the infrastructure needed to achieve conformity
Includes: buildings, utilities, hardware, software and communication

Server Room & Utilities

- Generators (back-up)
- UPS
- Cooling & HVAC
- Fire Protection
- Access Control
- Network switches

Software

- ERP (Enterprise Resource Planning) systems
- MRP (Material Requirements Planning) systems
- Mail server

Documented requirements for maintenance activities, including their frequency, records to be maintained.

- Equipment installed and maintained (records)
- Maintenance contracts
- Back-up frequency and location of data
- Disaster recovery

Audits

§ 7.3 D&D →

Standards & Data Integrity

Quality Management System Assessment

§ 7.3 Design and Development

D&D Inputs: Product description with specifications relating to intended use, configuration, composition, incorporated elements, and other design features

D&D Outputs: Enables verification against design output including acceptance criteria. Used for purchasing, production, inspection and testing.

D&D Verification & Validation: ensures outputs have met inputs. Ensures product is capable of meeting requirements for intended use.

D&D Changes: All changes identified and records maintained. Reviewed, verified and validated, as appropriate, and approved before implementation. *e.g.* ECN/ECO Engineering Change Notice / Engineering Change Order.

Records to be maintained

§ 8.2 M&M →

Standards & Data Integrity

Quality Management System Assessment

§ 8.2 Monitoring and Measurement

Internal Audit: ensures that the QMS is effectively implemented and maintained.

M&M of Processes: demonstrate the ability of the processes to achieve planned results.

M&M of Product: verify product requirements have been met.

- inspection/test procedure(s) and revision level used
- identify the test equipment used
- include test data
- be signed and dated by the person responsible for the inspection or test
- identify the number of products examined & the number of products accepted
- record the disposition of any products failing inspection or test, and the reasons for failure

Analysis of Data: Collect and analyse appropriate data to demonstrate the suitability and effectiveness of the quality management system

Records to be maintained

§ 4.2 Docs I →

Standards & Data Integrity

Quality Management System Assessment

§ 4.2.3 Control of Documents I

- responsibilities for preparation, approval and issue of documents
- ensure prompt withdrawal of obsolete copies of controlled documents
- define a method for recording the implementation date of a document change
- allow controlled and non-controlled documents to be distinguished

Document structure: title, scope, date of issue, effective date, revision and history, author, approver, pagination, distribution computer file reference.

Electronic documents: access, storage, reproducibility, readability, audit trails and electronic signatures

§ 4.2 Docs II →

Standards & Data Integrity

Quality Management System Assessment

§ 4.2.3 Control of Documents II

Changes to documents - reviewed and approved either by the original approving function or another designated function which has access to pertinent background information

Retention period **-** at least one copy of obsolete controlled documents shall be retained ensure that documents to which medical devices have been manufactured and tested are available for at least the lifetime of the medical device or as specified by relevant regulatory requirements*****.

**MDD 93/42/EEC: Period ending at least five years, and in the case of implantable devices at least 15 years, after the last product has been manufactured. Ref.: Annex II - VII*

§ 4.2 Recs I →

Standards & Data Integrity

Quality Management System Assessment

§ 4.2.4 Control of Records I

Records differ from documents

Provide evidence of conformity to the requirements:

- Design, manufacture, distribution and effective operation of the QMS

Properly identified, indexed filed, and readily accessible.

Stored safely, protected from unauthorized access, and protected from alteration.

Retention period - equivalent to the lifetime of the medical device, but not less than two years from the date of product release by the organization or as specified by relevant regulatory requirements*****.

**MDD 93/42/EEC: Period ending at least five years, and in the case of implantable devices at least 15 years, after the last product has been manufactured. Ref.: Annex II - VII*

§ 4.2 Recs II →

Standards & Data Integrity

Quality Management System Assessment

§ 4.2.4 Control of Records II

Electronic Records: consider retention times and take into account the degradation of the electronic data and the availability of devices and software needed to access the records.

Hand Written Records: made by indelible medium.
Include as appropriate:

- do not pre-date or post-date records
- do not use another person's initial, signature or equivalent
- complete all fields or check-offs when using a form
- verify all entries for completeness and correctness
- number pages to ensure completeness

Record Errors:
Paper records - should be corrected such that original entry maintained with the correction initialled and dated. Rationale for correction to be recorded where appropriate.
Electronic records – allow for audit trail for tracking changes.

QMS. Assess. e.g. →

Standards & Data Integrity

Quality Management System Assessment

Audit Examples

- New server installed in secure server room, old server removed and stored outside of secure room.
- Critical data/information stored on personal emails/local hard drive; uncontrolled.
- Incomplete records signed and approved.
- Batch of product located within warehouse. Batch record manually deleted from ERP system with note to file. In adequate control and traceability of product.
- Calibration records for monitoring/measuring device incomplete; device noted as being in use during audit.
- Records missing signatures or signed off at inappropriate level.

Thank you for your attention

NSAI Certification

HPRA

An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Data Integrity: A Regulator's Perspective

Ciara Turley – Health Products Regulatory Authority

2015 PDA Data Integrity Seminar

12th May 2015, The Hilton Hotel, Charlemont Place, Dublin 2

Presentation Content

- What is Data Integrity
- Elements in inspection focus
- Sample deficiencies

What is Data Integrity?

- Refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle and is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data
- Data is recorded exactly as intended, and upon later retrieval, the data is the same as it was when it was originally recorded

Data should be:

A – attributable to the person generating the data

L – legible and permanent

C – contemporaneous

O – original record or true copy

A – accurate

'Metadata' is the data about data and provides context and relationship to the primary data thus preserving the accuracy, completeness, content, and meaning.

Inspection focus

- EU Regulatory Requirements – Part I Chapter 4 and Annex 11 and Part II
- Data integrity requirements applicable to:
  - API and FP manufacturers, including contract manufacturing
  - Testing units, including contract laboratories
  - Outsourced GMP activities such as equipment qualification and calibration

Inspection focus - general

- Company understanding of computerised system capabilities and transfer of data between systems
- Up to date listing of all relevant systems and GMP functionality
- Control of networked & standalone instruments
- Policies and procedures detailing processing and control of data

Inspection focus - qualification

- User Requirement Specification - should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact.
- Evidence of appropriate test methods and test scenarios for parameter limits, data limits and error handling
- Justification on the extent of validation and data integrity controls documented through risk assessment of the computerised system.

Inspection focus – system administration

- Configuration of systems – GxP functions
- Security of the system and user access levels – appropriate segregation of duties
- Electronic signatures – use of individual and generic passwords

Inspection focus - data

- Data processing and review
- Accuracy checks
- Potential for data manipulation and deletion
- Repeat testing / replicate data
- Date / time stamp manipulation
- Criteria used to invalidate data
- Data transfer to systems - Checks that data are not altered in value and/or meaning (primary and meta data). Level of checking should be statistically sound

Inspection focus – storage of data

- Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.
- Archived data should be checked for accessibility, readability and integrity. If changes are to be made to the system, then the ability to retrieve the data should be ensured and tested

Inspection focus

- Audit trails - Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions
- Vendors - Subject to Chapter 7 requirements, assessment of competency of contractor to deliver expectations.
- Change management - Changes to a part of the system may pose a risk due to interdependencies.

Inspection focus

- Data Integrity included in risk assessments
- Data Integrity included in training programme
- Data Integrity included in self inspection programme - justify frequency of periodic evaluation based on system criticality and complexity

Deficiencies - Computerised Systems

- A listing of GMP computerised systems was not maintained.
- The software utilised to control [equipment] had not been categorised.
- Not all critical GxP systems were present. For example the [Equipment] Program and Review software.
- While a statement of GxP or non-GxP was documented for Global Systems, there was no associated documentation justifying the statement.
- Computerised System Risk Assessments for critical systems were not in place.
- There was no system description/boundary despite the critical system being ‘live’.

Deficiencies - User Accounts

- It was possible for administrators to verify their own test result recording in ERP. There were no procedural restrictions around this and was hence considered to increase the overall risk of the associated testing processes.
- The ‘system owner access level’ was not described.
- The removal of test accounts had not been considered by the company prior to the system going ‘live’.
- [ERP] access configurations for the job roles within the site was not adequately defined in that there was no documented correlation of roles to the user access elements defined by the Global [ERP] group.
- System authorization concepts were not always considered in that Users could be administrators with full system access and also have batch manufacturing responsibilities.

Deficiencies - Audit Trails

- Audit trail comments on [the CDS] were not always sufficiently detailed. For example, a number of changes were observed to have been made to the integration method utilised on [a test] on [a date] and these had a comment of 'save' documented.
- Operating System User Accounts were utilised to access the <system>. There was no periodic review of Operating system audit trails (logs) as appropriate and this was not justified.

Deficiencies - Qualification

- The qualification of the ERP system was considered deficient in that:
  - The independent code review was not available for review during the inspection.
  - The actual observed results were not always documented within the qualification records
  - The procedure for electronic signatures data transfer to the ERP system was not described in a procedure and was not qualified.
  - There was no assessment of ERP database integrity.
- The decision not to test requirement [Electronic Signatures] documented in [Rationale] was not considered to be justified in that the referenced documents disclaimer stated that the information should not be relied upon.

Deficiencies - Qualification

- The Virtual Private Network software had not been subject to GxP assessment or qualification as appropriate.
- In relation to the back up and restoration of data
  - There was no process for logging of media used to back up the server systems.
  - The maximum number of uses for the magnetic tapes was not defined or the number of uses controlled.
  - All backup activities on the site were not procedurised. For example back up of the [Program] data from [Equipment] and back up of certain [Equipment] PLC code was performed on an ad-hoc basis using HDDs which were not stored in an appropriate location.

Deficiencies - Periodic Evaluation

- The periodic assessment of computerised systems had not been completed for all equipment. For example, [computerised system] was installed [a long time ago] and at the time of the inspection had not been reassessed.
- Periodic review of global applications was not performed and there was no procedure in place for periodic review.
- The periodic system review of the <system> was <documented>. The review stated that there was no requirement for audit trail review as they were “displayed on the screen”. This was not considered to justified. Further to this, there was no procedure in place for periodic audit trail review.

Deficiencies - Change Management

- In relation to the testing associated with <IT Change Control System>, the evidence for the appropriate test scenario was not available for review. The system permitted only the most recent test scenario for the process to be viewed. There was no evidence that the system level risk assessment had been critically assessed prior to this change in order to determine the appropriate test scenarios. Further to this, the change to this production parameter had been assigned as a non regulatory change i.e. not subject to GxPs.
- Change logs for <ERP> user access sub-role profiles were maintained in an uncontrolled manner. E.g Z_XXX_XXX_XX_DATA, the associated text box change log had three entries post implementation of <IT Change Control System> whereas <IT Change Control System> listed four valid changes for this profile

Deficiencies - Production

The following deficiencies were noted with regards to the blister packaging machine

- There was no controlled recipe in place to confirm that parameter settings on the machine were those approved.
- The time on the HMI was incorrect – the actual time (taken from the wall clock in the packaging area was recorded at 12:15, the machine time was displayed as 11:08.
- A generic operator password was in use
- Audit trails were not reviewed.
- The print out function was not enabled and there was no assessment to determine if stored data could be securely transferred or downloaded to storage media in an intelligible format for review
- Manufacturing data since 2003 from a previous manufacturer / owner was retained on machine.

Deficiencies - Production

The qualification and data integrity controls for the filling machine were considered inadequate in that:

- There was no technical agreement with the vendor
- A single generic user name and password was used to access and operate the equipment.
- The time setting on the software control was inaccurate.
- The audit trail could not be generated at the time of inspection.
- The system and security for archiving of data was not known
- The User Requirement Specification did not specifically state all the requirements for the machine and was not linked to any critical process parameters / variables

Deficiencies - Production

- The company is advised that manufacturing controls should be updated in line with technical progress (ref. Directive 2003/94/EC, Article 5 (2)). In particular fluid bed dryers should be equipped with chart recorders to facilitate monitoring and recording of the granulate drying process.
- The qualification / revalidation was deficient in that there was no consideration of the impact of updated requirements since the initial IOQ, specifically Annex 11.

Deficiencies - Production

- In relation to Filter Integrity Testing:
  - There were no controls around the number of repeat FITs that could be performed in the event of a filter failure for either product or vent filters.
  - There was no requirement to reconcile the number of tests reported versus the number of tests performed on the Pall units.
  - Failed FIT runs were not recorded on form X although the form required a ‘Pass/Test’ result to be recorded.

Deficiencies - QC data

- There was no justification for the test injections of samples including stability samples being run prior to system suitability.
- There was no explanation for why areas changed for test injections from test, test 1 and test 2, prior to running the sample set. It was noted that when the assay for test was calculated that this resulted in an OOS result, whereas the result for test 2 was within specification.
- The Empower list of users and user types did not reflect the highest level of access a user had.
- Analysts with System Administrator access had the ability to change custom fields including calculations and sample names.

Deficiencies - QC data

- The company stated that sample injections were being run as there were problems with the systems, however; no evidence of this was presented.
- The results of a processed test injection had been deleted by an analyst with administrator access.
- There was no requirement to review raw data on electronic systems.
- There was no requirement to review audit trails.
- Projects were not locked and it was possible to reprocess results

Deficiencies - QC data

- There was no date / time stamp of printing on analytical reports from ‘system’ (chromatograms, methods and sample set data) to facilitate traceability and ensure integrity of the data
- The procedure for test performance and review of documents did not make reference to review of the audit trail or review of soft copies of the chromatograms on the ‘system’ network
- A number of sample sets and their associated injections on the ‘X system’ in the stability laboratory, were not all appropriately identified and carried non descriptive titles, such as “trial”

Deficiencies - QC data

- No deviations or explanations had been documented for a number of ‘altered sample’ incidences which were evident from ‘X system’ project audit trails
- There was no date / time stamp of printing on analytical reports from ‘X system’ (chromatograms, methods and sample set data) to facilitate traceability and ensure integrity of the data
- The procedure for test performance and review of documents did not make reference to review of the audit trail or review of soft copies of the chromatograms on the ‘X system’ network
- Alterations to runs were frequently performed to add an extra test or blank sample but there was no procedure in place for this and the reason for the changes was generally not recorded to a level of detail enabling the true reason for the change to be determined

Deficiencies - QC data

- A number of sample sets and their associated injections on the 'X system' in the stability laboratory, were not all appropriately identified and carried non descriptive titles, such as "trial"
- Management of the 'X system' was considered deficient as a number of GxP functions were observed as not switched on (e.g. Allow lock channels after sign off, Disallow use of Annotation Tools etc). In addition, it was observed that a statement by 'X company' reflected below the GxP function window indicated that they recommended all GxP functions to be switched on
- The LC Solution system (version 'y.yyy') for the 'X' HPLC system was considered deficient in that all users could gain 'Administrator' access to the application system by using a common username 'Admin' and no password

Deficiencies - QC data

- Raw data for HPLC/GC runs which had been invalidated due to failed system suitability criteria were stored separately to the QC raw data packages and were not included in the review process. The 'log for record of invalidated runs' was not incorporated under the quality management system and invalidated runs were not always evaluated and documented
- Original run sequences which had been amended during HPLC/GC runs were not printed and retained with the QC raw data packages
- Full Audit Trail did not appear to be available for the 'X' data acquisition system in that the different version numbers of the processing methods were not all visible in the audit trail (e.g. the current version of 'Y' method was 18 and only 7 lines were visible on the audit trail). In addition, there were no data audit trails available on this system

Deficiencies - QC data

- For IT personnel with administrator rights it was possible to copy, rename or delete files (i.e. chromatograms and metafiles) in the system without it being tracked in an Audit Trail
- The process of review of HPLC analytical data packages by the QC checker does not require a formal review of the electronic raw data or a review of the audit trails for the processing method and instrument method associated with the analysis sequence. In the examples reviewed printouts of processing methods were not included with the QC raw data packages for review
- There was no requirement for electronic review of GC analytical data & relevant audit trails to be conducted during the review and approval of QC data. In addition, the QC/QA reviewers did not have access rights to the 'X' systems in order to conduct such reviews

Deficiencies - QC records

- Entries made in training records, production logbooks and QC records were made by staff that the company biometric logging in record showed were not on site at the time that the entry was purported to have been made
- QC equipment records logged the use of a specific HPLC column for testing performed on site at a time when other records showed that the same column had been transferred to a contract testing laboratory
- Evidence of deleted TOC data files were noted. An analysis file from ‘xxx’ date was observed in the deleted files/recycle bin of the computer. A duplicate analysis file for the same samples on the same day was found within the file structure. There was no reference to the second file or any file deletion either in the test records or the system logbook and no explanation was offered during the inspection

Deficiencies - QC equipment

- The control of un-networked equipment (UV and TOC) in the QC laboratory was deficient in that:
  - A number of data discrepancies were noted in the system file structure
  - Repeated and unlabelled testing data folders and test packages were observed
  - At the time of the inspection the company could not fully explain the discrepancies noted
  - Software had not been qualified or validated to demonstrate that the key functionality of the system functioned as required

Deficiencies - stability

- Stability data had discrepancies including:
  - Initial records of secondary spots for TLC related substance tests were later re-annotated to indicate that no secondary spot had been identified
  - Data recorded in summary reports were not reflective of the raw data
  - Summary reports were presented to the inspector for which the supporting raw data could not be provided
  - Missing raw data and summary report for batch of ‘X’ Tablets where stability data had been used to support the risk assessment of product remaining on the market in the EU
  - Missing raw data and incorrect entries that were reviewed and authorised as correct
  - Some stability data presented to the inspector was from product packed in different packaging to that supplied to the market and therefore not relevant

Deficiencies - stability

- Stability data had discrepancies including:

- Initial records of secondary spots for TLC related substance tests were later re-annotated to indicate that no secondary spot had been identified
- Data recorded in summary reports were not reflective of the raw data
- Summary reports were presented to the inspector for which the supporting raw data could not be provided

Deficiencies - stability

- Stability data had discrepancies including (cont'd):

- Missing raw data and summary report for batch of 'X' Tablets where stability data had been used to support the risk assessment of product remaining on the market in the EU
- Missing raw data and incorrect entries that were reviewed and authorised as correct
- Some stability data presented to the inspector was from product packed in different packaging to that supplied to the market and therefore not relevant

EudraGMDP – Statements of Non-compliance

- Issues identified which compromised the integrity of analytical data
  - Evidence seen of data falsification
  - Significant number of product stability data results reported in the Product Quality Reviews had been fabricated
  - Neither hard copy nor electronic records available
  - Issues seen with HPLC electronic data indicating unauthorised manipulation of data and incidents of unreported trial runs prior to reported analytical runs
  - Record integrity and veracity - some records made up or altered
  - Lack of mechanisms to ensure integrity of analytical data

EudraGMDP – Statements of Non-compliance

- Critical deficiency cited with regards to testing of finished product and stability testing related to data integrity
  - Deleted electronic files with no explanation
  - The running of "trial testing" prior to performing system suitability and the formal testing
  - Loss of control of reconciliation of samples - those used for additional testing could not be traced
  - Manipulation and falsification of documents and data observed in different departments

Summary

- You don’t need to be an IT expert, but you need to know GMP requirements
- Understand the capability of your equipment, know if it stores electronic data, assess if parameters are changed what impact it will have.
- Integrity of data is not a ‘new’ regulatory requirement.

References:

- EU Guidelines to GMP Part I and II
- EMA Questions and Answers: Good manufacturing practice
- MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015
- HPRA presentations
  - GMP information Day November 2014,
  - Trinity QP Forum 2014 and 2015,
  - ISPE GAMP Seminar April 2015

VALIDANT
Vital in healthcare

Data Integrity; An Industry Perspective

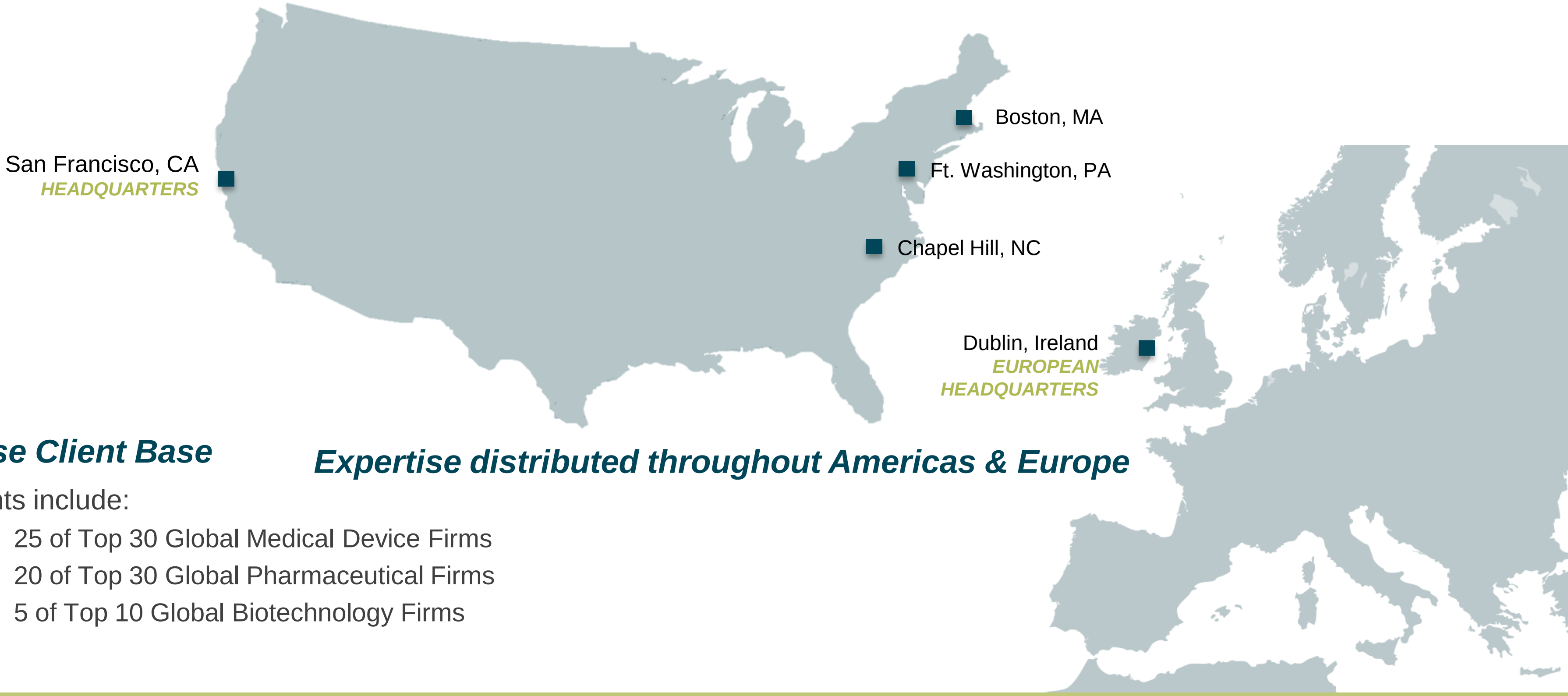
Brian O’ Broin

VP European Operations, Validant

Validant Background

Validant is a global life-science services firm with a focus on the functional areas of Quality, Regulatory Affairs, Manufacturing, and Engineering. We blend best practices of Strategic Consulting and Professional Services to create deliverables-based solutions for our clients.

Founded in 2005, Current Office Locations Include…



Expertise distributed throughout Americas & Europe

Diverse Client Base

- Clients include:
  - 25 of Top 30 Global Medical Device Firms
  - 20 of Top 30 Global Pharmaceutical Firms
  - 5 of Top 10 Global Biotechnology Firms

Key Functional Areas

Compliance & Quality Systems Support

Risk Assessment

Assessment , Development & Implementation of Quality Systems / Standards

Compliance Audits / PAI

Investigations / CAPA Process & Support

Quality Engineering

Manufacturing & Laboratories

Technical Transfer

New Product Introduction

Lab. Data & Systems Review

Validation:

Equipment & Process

Facilities & Utilities

Cleaning Validation

Test Method Validation

CSV

Regulatory Consulting Services

Regulatory Response Development

Remediation Planning & Execution

Submission Support & CMC Authoring

Post Market Surveillance

Complaints Reporting

Annual Reporting Support

PAI Assessment & Strategy

Regulatory Strategy

Resources: On site project management, technical expertise, project consultants, staff augmentation, etc.

Resources: Deliverable-based outcomes completed by high-level expertise

Data Integrity; An Industry Perspective

Presentation Content

- Brief Introduction to Validant
- Change in Industry Focus
- What is Data Integrity
- Regulatory Requirements
- Impact of an absence of Data Integrity
- Data Integrity – A Global Issue
- Importance of India
- Breaches of Data Integrity
- Some Causes & Action if Identified
- Questions

VALIDANT
Vital in healthcare

Data Integrity (DI) - Regulatory Focus

Change in Regulatory Focus

The integrity of the data collected and recorded by pharmaceutical manufacturers is critical to ensuring that high quality and safe medicines are produced.

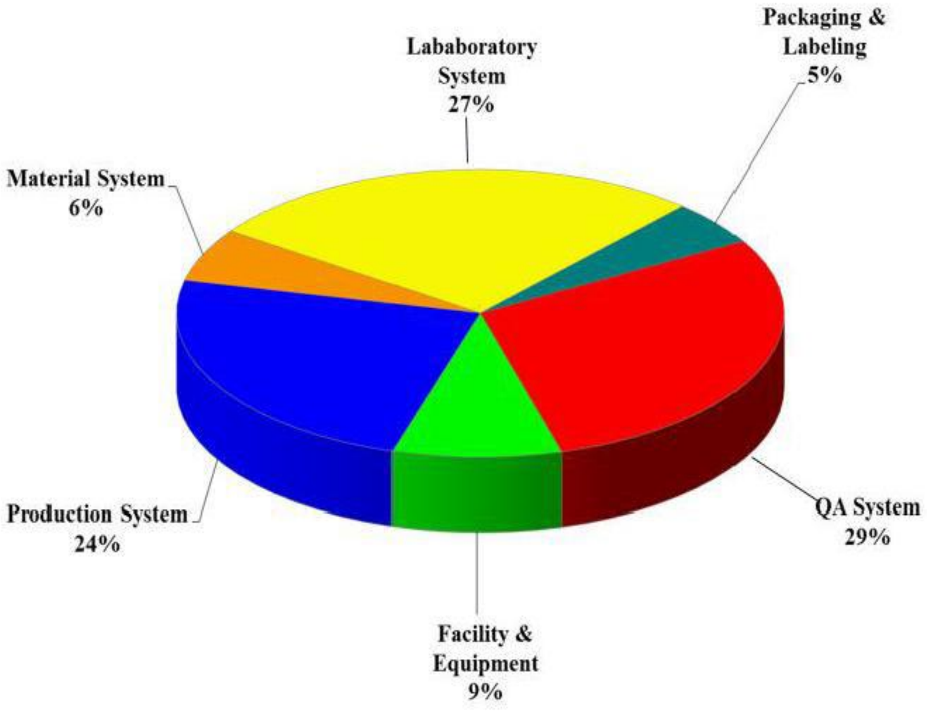
International Regulatory focus has shifted to DI issues and between 2010 & 2013 US FDA, WHO & UK MHRA inspectors have undergone training to better detect signs of data problems.

Regulatory authorities are looking more closely at international facilities for signs of altered and doctored records.

The existing EU GMP guidelines and 21 CFR, Part 210 and Part 211 have amongst others provisions for identifying DI issues.

Data Integrity - Regulatory Focus

12 out of 13 FDA Warning letters issued between November 2013 to July 2014 (to non US sites) had Data integrity issues as against 8 out of 26 in previous year.



Data integrity is a lingering problem that is not going away!

Regulatory Requirements:

EudraLex - Volume 4, GMP Guidelines, Annex 11

General:

1. Risk Management

"Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system."

Regulatory Requirements

EU GMP CHAPTER 1	EU GMP Chapter 4
<u>Chapter 1 - Pharmaceutical Quality System</u> ***<u>Quality Control 1.9</u>*** *1.9 (iv) Records are made, manually and/or by recording instruments, which demonstrate that all the required sampling, inspecting and testing procedures were actually carried out. Any deviations are fully recorded and investigated;*	***<u>Chapter 4 - Documentation</u>*** ***<u>Retention of Documents</u>*** *4.10 It should be clearly defined which record is related to each manufacturing activity and where this record is located. Secure controls must be in place to ensure the integrity of the record throughout the retention period and validated where appropriate.*

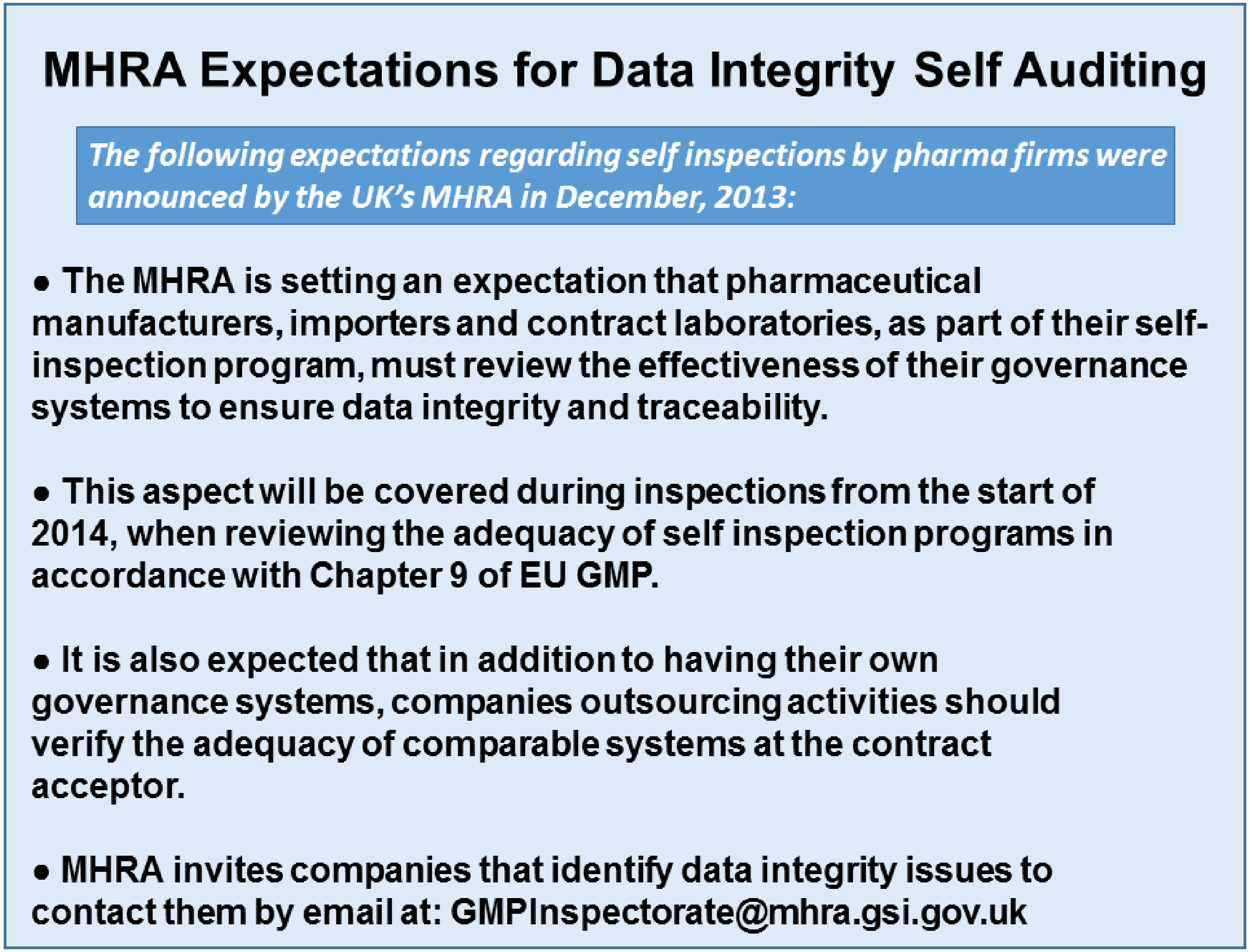
VALIDANT
Vital in healthcare

Regulatory Requirements

EU GMP Chapter 6	US FDA – 21 CFR
Chapter 6 – Quality Control General : ➢ *6.1 Independent Quality Control Department* *Documentation:* ➢ *6.7 Laboratory Documentation* ➢ *6.9 Trending of Data* ➢ *6.10 Laboratory Note Books* *Testing:* ➢ *6.15 Validation of Analytical Methods* ➢ *6.16 Recording and checking of results* ➢ *6.17 Recording of details of test performed* ➢ *6.18 Testing and reporting results of In-process Samples*	*FDA 21 CFR PART 211* *Subpart J – Records and Reports* ➢ *Sec. 211. 180 General Requirements* ➢ *Sec. 211.182 Equipment Cleaning and use log* ➢ *Sec.211. 184 Component, drug product container, closure, and labeling records.* ➢ *Sec 211.186 Master Production and Control Records* ➢ *Sec 211.188 Batch production and control records.* ➢ *Sec 211.192 Production record view* ➢ *Sec 211.194 Laboratory records* ➢ *Sec 211. 196 Distribution records* ➢ *Sec 211.198 Complaint files*

VALIDANT
Vital in healthcare

Regulatory Requirements



MHRA Expectations for Data Integrity Self Auditing

The following expectations regarding self inspections by pharma firms were announced by the UK's MHRA in December, 2013:

- The MHRA is setting an expectation that pharmaceutical manufacturers, importers and contract laboratories, as part of their self-inspection program, must review the effectiveness of their governance systems to ensure data integrity and traceability.

- This aspect will be covered during inspections from the start of 2014, when reviewing the adequacy of self inspection programs in accordance with Chapter 9 of EU GMP.

- It is also expected that in addition to having their own governance systems, companies outsourcing activities should verify the adequacy of comparable systems at the contract acceptor.

- MHRA invites companies that identify data integrity issues to contact them by email at: GMPInspectorate@mhra.gsi.gov.uk

What is Data Integrity:

Data Integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle. It is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data;

Data is recorded exactly as intended, and upon later retrieval, the data is the same as it was when it was originally recorded

Data is complete, consistent & accurate;

According to FDA, which uses the acronym **ALCOA**, data need to be "attributable, legible, contemporaneous, original, and accurate."

Data Integrity : ALCOA

Attributable	**Who performed an action and when? If a record is changed, who did it and why? Link to the source data.**
Legible	Data must be recorded permanently in a durable medium and be readable.
Contemporaneous	The data should be recorded at the time the work is performed and date / time stamps should follow in order
Original	Is the information the original record or a certified true copy?
Accurate	No errors or editing performed without documented amendments.

VALIDANT
Vital in healthcare

Ensuring Data Integrity

Protect original data from

- Accidental Modification
- Intentional Modification
- Falsification
- Deletion

Impact of absence of Data Integrity:

What happens when data integrity is breached?

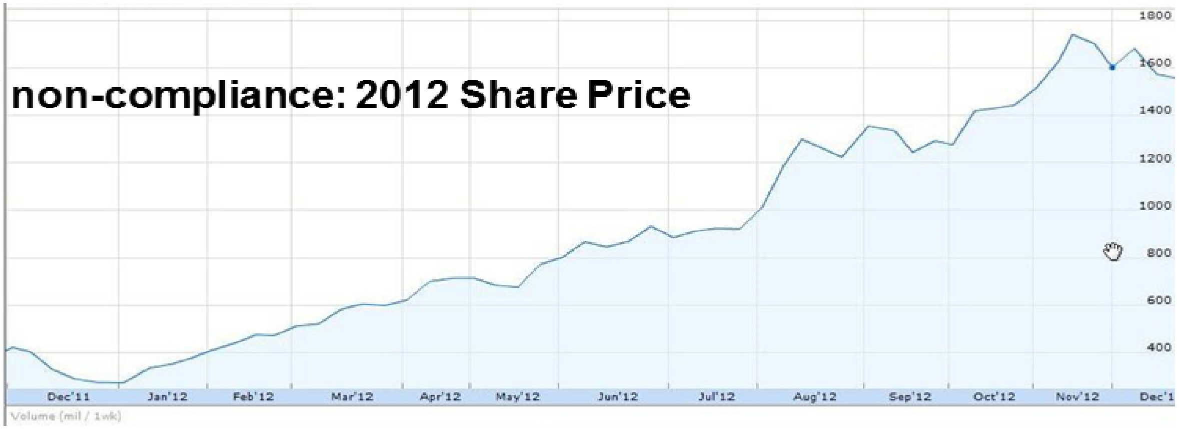
In many cases, Pharma Companies have been impacted by:

- Consent Decrees
- FDA Warning Letters
- EU statements of non-compliance (SNC),
- Importation Ban(s)
- Loss of consumer confidence
- Product applications review suspended
- Market & share price reduction

MHRA GMDP Inspections Group Manager Mark Birse provided an analysis of the impact of data integrity observations on the market value of a firm.

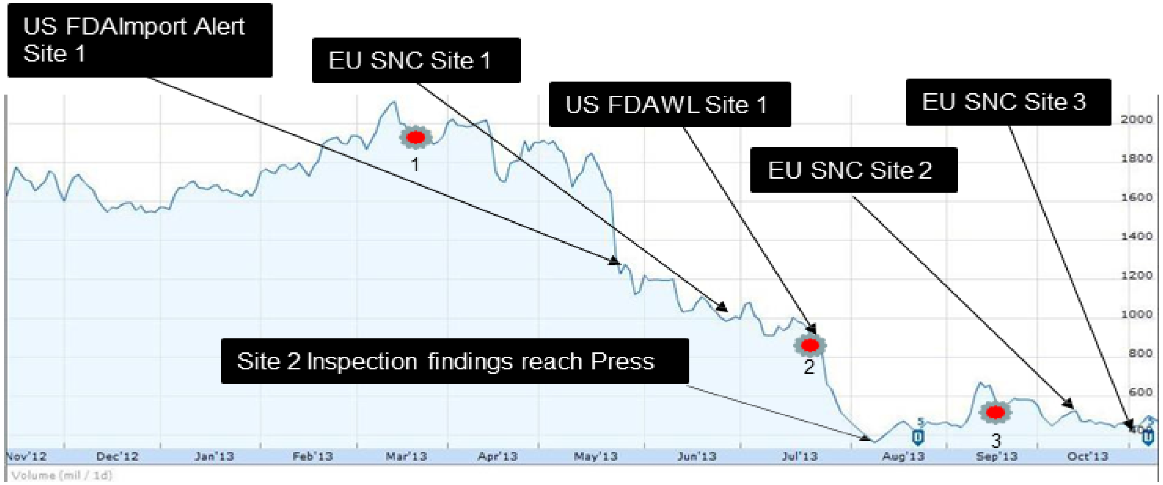
Cost of non-compliance: 2012 Share Price

Share price for the firm involved had quadrupled during 2012.



Share price during 2013

As inspections revealed deficiencies that resulted in FDA import alerts and EU statements of non-compliance (SNC), the value of the company declined rapidly


US FDAImport Alert Site 1

EU SNC Site 1

US FDAWL Site 1

EU SNC Site 3

EU SNC Site 2

Site 2 Inspection findings reach Press

"….Imagine if a small slice of that (share value) had been taken off and been spent on quality – actually doing the right thing.."

VALIDANT
Vital in healthcare

Impact of absence of Data Integrity:

The worst case scenario is impact on patient safety and the loss of lives.

Although not regulated by the FDA or subject to cGMPs, the New England Compounding Pharmacy incident in the US (MA) in 2012 can be used as an example of the consequences of data related fraudulent activity.

In this case, 17,000 vials of methylprednisolone for injection contaminated with fungi were distributed to 23 US states.

Resulted in 64 patients deaths and over 750 who suffered illness with fungal meningitis as a result of sterility negligence & data integrity issues.

In this case, a FDA official said pharmacy technicians were instructed to lie on cleaning logs, showing rooms as being cleaned when they had not. This was undertaken per instruction of management.

Data Integrity issues are a Global problem

Carmelo Rosa, Director of FDA OMPQ’s (Office of Manufacturing & Product Quality),recently acknowledged that “*Data integrity issues have always existed!”,* but now FDA is doing more to uncover the evidence of such problems.

Drug makers should not look to contract manufacturers to reduce their responsibility for data accuracy and reliability, Some biopharma companies regard contract testing and production operations as one way to alleviate their involvement in inspections and dealings with regulatory authorities.

But Rosa emphasized that the licensed manufacturer remains responsible for products meeting all quality standards and noted that FDA and other authorities are looking closely at all facilities, including CMOs.

Although a Global issue, many of the most egregious data integrity transgressions have surfaced at Indian API & finished product manufacturing facilities.

Ref. WL: 320-14-01

Wockhardt Ltd. was cited in a July 2013 WL for multiple GMP violations, including efforts to cover up faulty and incomplete anti-microbial studies, stability protocols, and batch testing.

FDA stated:

‘….on March 18, 2013, the FDA investigators found unofficial batch records for approximately 75 batches of injectable finished drug products torn in half in a waste area. These records contain data indicating that some batches failed to meet the in-process visual inspection specifications of not more than ***(b)(4)****% defects, while the official batch records for these batches state that these batches had met the specifications…’*

The uncontrolled documents indicate that up to 14% of vials had defects including, but not limited to, black particles, fibers, glass particles, sealing defects, and volume variations.

Ref. WL: 320-14-01

‘The FDA investigators identified the practice of performing "trial" sample analysis for High Performance Liquid Chromatography (HPLC) analyses prior to collecting the “official” analytical data for stability testing. These “trials” were performed on multiple products, including ***(b)(4)*** *Tablets* ***(b)(4)****mg,* ***(b)(4)****mg/****(b)(4)****ml, and* ***(b)(4)****Tablets. These trial runs were not recorded in the equipment use log, and sample preparation data associated with these analyses was destroyed, preventing any calculation or analysis of the resulting data.’*

FDA concluded:

‘…The above examples raise serious concerns regarding the integrity, reliability and accuracy of the data generated and available at your facility. ’

Warning Letters FDA – issued to Indian pharma companies for data integrity related issues

Warning Letter Issued To	Warning Letter Issue Date
Apotex Research Private Limited	01/30/2015
Micro Labs Limited	01/09/2015
Cadila Pharmaceuticals Limited	10/15/2014
Marck Biosciences Ltd.	07/08/2014
Apotex Pharmachem India Pvt Ltd.	06/17/2014
Sun Pharmaceutical Industries	05/07/2014
Canton Laboratories Private Limited	02/27/2014
USV Limited	02/06/2014
Wockhardt Limited	11/25/2013
Agila Specialties Private Limited	09/09/2013
Posh Chemicals Private Limited	08/02/2013
Aarti Drugs Limited	07/30/2013
Wockhardt Limited	07/18/2013
Fresenius Kabi Oncology Ltd	07/01/2013
RPG Life Sciences Limited	05/28/2013

Last updated on 3 February 2015

VALIDANT
Vital in healthcare

Importance of India

A leading global provider already

- World's 3rd largest generics producer

- Produces 10% of world's medicines

- Over US $12 Billion exports to 200 countries

- 41% of U.S prescriptions are manufactured in India

- 23% of UK product Licenses name an Indian manufacturer
& 38% an Indian API source

- Large and growing base of educated raw talent
- Skilled chemists, chemical engineers and Ph.Ds at 1/6th to 1/3rd of U.S. costs
- Large and diverse patient pool

In 2013, there were 4,655 pharmaceutical manufacturing plants in India, employing circa 350,000 people.

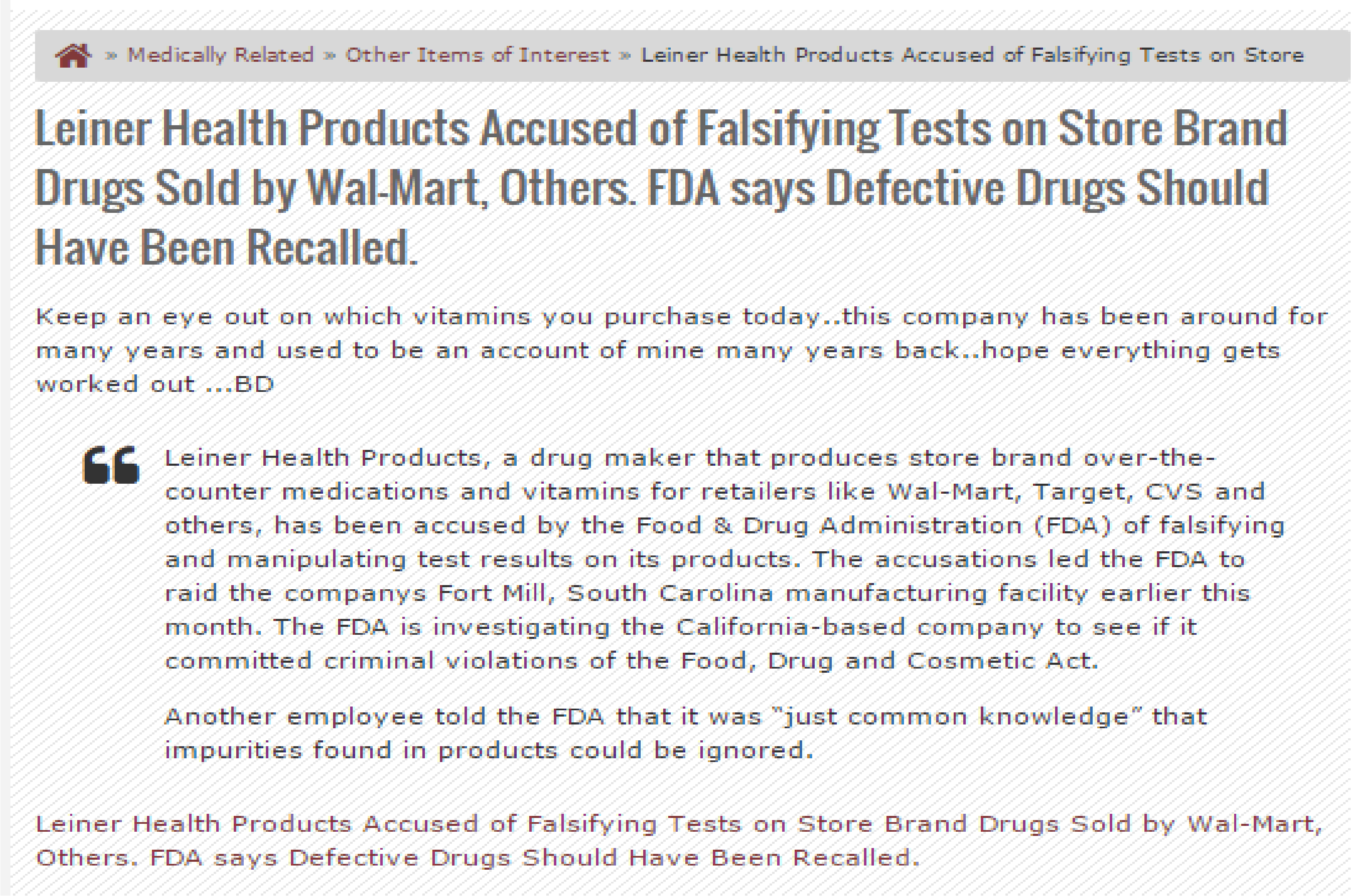
Warning Letters by FDA – Company rank in India within Top 20

Warning Letter Issued To	Warning Letter Issue Date
Apotex Research Private Limited	01/30/2015
Micro Labs Limited (18)	01/09/2015
Cadila Pharmaceuticals Limited (7)	10/15/2014
Marck Biosciences Ltd.	07/08/2014
Apotex Pharmachem India Pvt Ltd.	06/17/2014
Sun Pharmaceutical Industries (1) *	05/07/2014
Canton Laboratories Private Limited	02/27/2014
USV Limited(20)	02/06/2014
Wockhardt Limited (6)	11/25/2013
Agila Specialties Private Limited	09/09/2013
Posh Chemicals Private Limited	08/02/2013
Aarti Drugs Limited	07/30/2013
Wockhardt Limited (6)	07/18/2013
Fresenius Kabi Oncology Ltd	07/01/2013
RPG Life Sciences Limited	05/28/2013

- April 2014 Announcement that Sun Pharmaceuticals would be acquiring Ranbaxy Laboratories.

VALIDANT
Vital in healthcare

A global problem



» Medically Related » Other Items of Interest » Leiner Health Products Accused of Falsifying Tests on Store

Leiner Health Products Accused of Falsifying Tests on Store Brand Drugs Sold by Wal-Mart, Others. FDA says Defective Drugs Should Have Been Recalled.

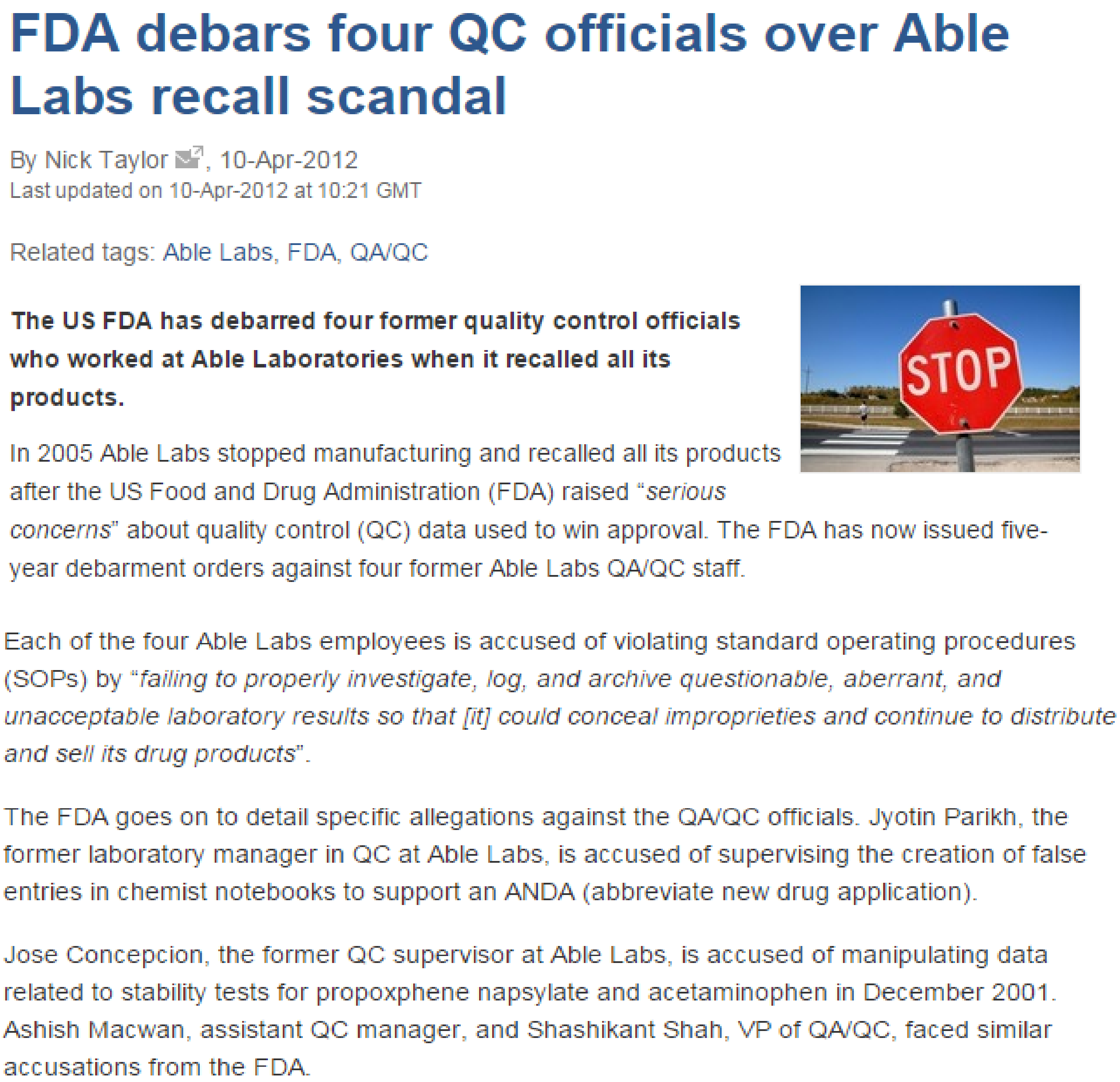
Keep an eye out on which vitamins you purchase today..this company has been around for many years and used to be an account of mine many years back..hope everything gets worked out ...BD

> Leiner Health Products, a drug maker that produces store brand over-the-counter medications and vitamins for retailers like Wal-Mart, Target, CVS and others, has been accused by the Food & Drug Administration (FDA) of falsifying and manipulating test results on its products. The accusations led the FDA to raid the companys Fort Mill, South Carolina manufacturing facility earlier this month. The FDA is investigating the California-based company to see if it committed criminal violations of the Food, Drug and Cosmetic Act.
>
> Another employee told the FDA that it was "just common knowledge" that impurities found in products could be ignored.

Leiner Health Products Accused of Falsifying Tests on Store Brand Drugs Sold by Wal-Mart, Others. FDA says Defective Drugs Should Have Been Recalled.

VALIDANT
Vital in healthcare

A global problem



FDA debars four QC officials over Able Labs recall scandal

By Nick Taylor, 10-Apr-2012
Last updated on 10-Apr-2012 at 10:21 GMT

Related tags: Able Labs, FDA, QA/QC

The US FDA has debarred four former quality control officials who worked at Able Laboratories when it recalled all its products.

In 2005 Able Labs stopped manufacturing and recalled all its products after the US Food and Drug Administration (FDA) raised "*serious concerns*" about quality control (QC) data used to win approval. The FDA has now issued five-year debarment orders against four former Able Labs QA/QC staff.

Each of the four Able Labs employees is accused of violating standard operating procedures (SOPs) by "*failing to properly investigate, log, and archive questionable, aberrant, and unacceptable laboratory results so that [it] could conceal improprieties and continue to distribute and sell its drug products*".

The FDA goes on to detail specific allegations against the QA/QC officials. Jyotin Parikh, the former laboratory manager in QC at Able Labs, is accused of supervising the creation of false entries in chemist notebooks to support an ANDA (abbreviate new drug application).

Jose Concepcion, the former QC supervisor at Able Labs, is accused of manipulating data related to stability tests for propoxphene napsylate and acetaminophen in December 2001. Ashish Macwan, assistant QC manager, and Shashikant Shah, VP of QA/QC, faced similar accusations from the FDA.

A global problem

Data integrity issues have surfaced in all regions. For example in the last 12 months

In June 2014**, Tianjin Zhogan Pharmaceutical Co.** in China received a warning letter citing inadequate records pertaining to manufacturing and cleaning operations (1).

A July 2014 warning letter, cited Italian API producer **Trifarma S.p.A**. for deleting key test data and failing to establish systems to identify how and when changes are made in manufacturing records.

In March 2015, **Hospira S.p.A.**, obtained a WL for their facility located at Via Fosse Ardeatine 2, Liscate, Italy. Some HPLC files had been deleted, while other backup files had been ‘overwritten’.

What is Breach of Data Integrity (BDI) ??

Breach of Data Integrity is , a violation of the integrity of Data. Which means, the actions performed and the documents/records written do not reflect the truth and the reality which has taken place.

It is not about Lab Data alone
“Data Integrity is not only about the QC, it applies to compliance with GMPs:

Relates to:

- **Research & Development**
- **Clinical Trials**
- **Manufacturing & Testing**
- **Inspection**
- **Post Inspection Activities**

Many Common Data Integrity Issues Found in Chemistry Laboratories:

Audit Trails – For electronic data acquisition systems, audit trails are not available or are not enabled; therefore, there is no record of data modifications or deletions.

Unique User Logins – Each user should have a unique username and password for both the analytical software and the operating system. This is essential for tracing work performed to a unique individual.

User Privilege Levels – Each data acquisition system should have defined user levels based on the role the user will have in the system. Examples of common user levels include analyst, supervisor, manager and administrator. Privileges assigned to each level should be clearly defined and commensurate with the requirements for each user type.

Test Non Compliant - Reporting on a CoA that batches meet test specification without actually performing the testing, or having any supporting data

Common Data Integrity Issues Found in Chemistry Laboratories cntd.

Control Over Electronic Systems – Failure to establish adequate controls over computer systems to prevent unauthorized access or changes to electronic data. This can include failure to have mechanisms to prevent unauthorized user access to the system, and ability to rename, move, delete or not save file results.

Control Over Processing Methods – Use of HPLC processing methods (including integration parameters) that are not defined or controlled. This includes the practice of manual integrations without justification or approval, and processing injections in the same sequence with different processing methods and integration parameters.

Unofficial "Test" Injections – Some firms have been cited for injecting samples prior to beginning an official sequence. This practice results in essentially generating data for products, but not reporting the data.

Common Data Integrity Issues (Non Laboratory):

operations personnel performing manufacturing steps without a batch record or a manufacturing form to document the results contemporaneously.

Manufacturing batch records IPC checks ‘completed’ in advance of a testing interval

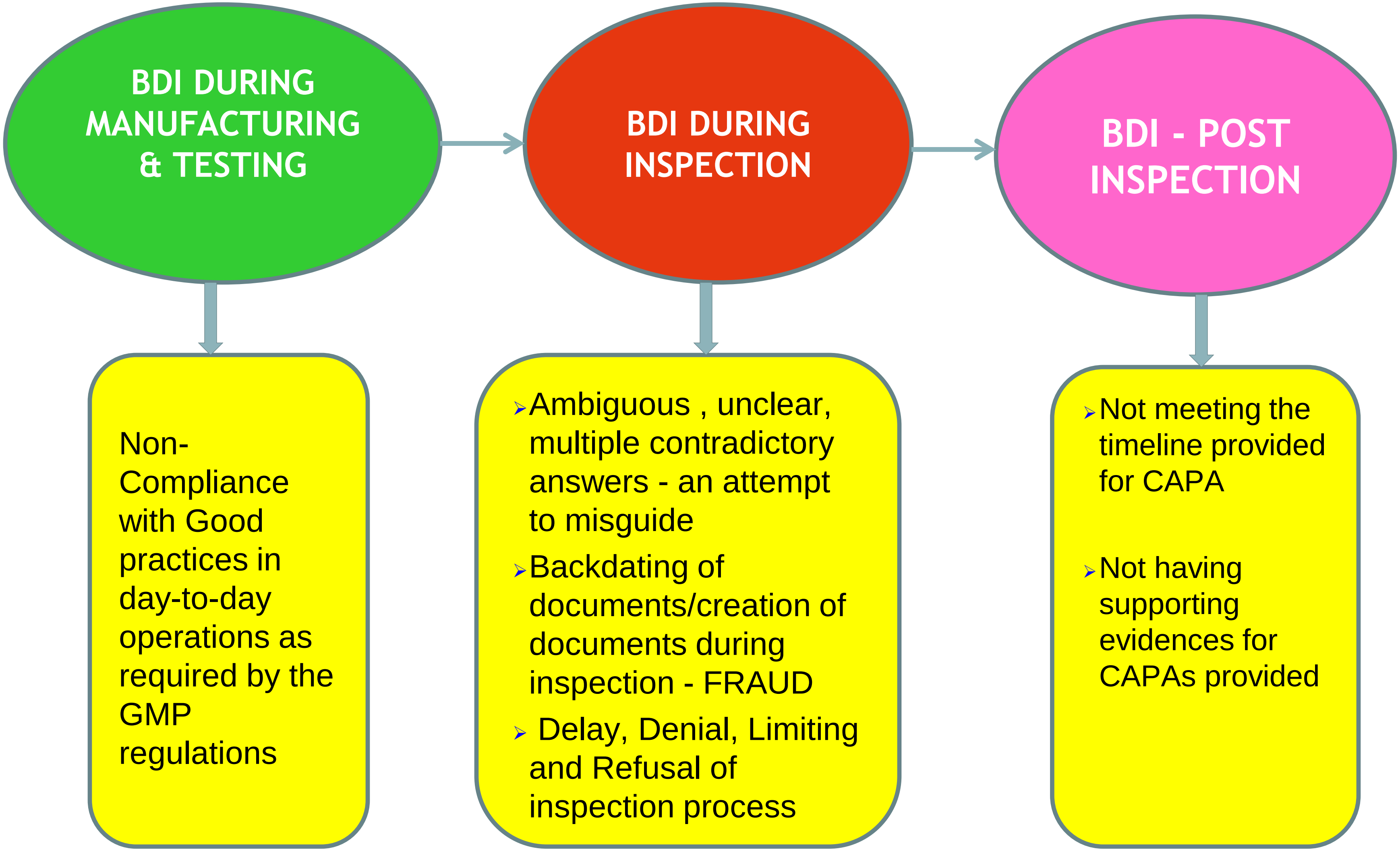
Manufacturing personnel back dating official documents & signing on behalf of each other.

Company maintaining duplicate versions of cGMP raw data records. Undesirable data was found to be changed in the official versions in order to meet specifications

using post-it notes to capture information and then transferring that to worksheets or formal documentation.

Blending API lots that had failed degradant testing with lots that had passed in order to obtain ‘in specification’ test results

Data Integrity



BDI DURING MANUFACTURING & TESTING

Non-Compliance with Good practices in day-to-day operations as required by the GMP regulations

BDI DURING INSPECTION

- Ambiguous , unclear, multiple contradictory answers - an attempt to misguide
- Backdating of documents/creation of documents during inspection - FRAUD
- Delay, Denial, Limiting and Refusal of inspection process

BDI - POST INSPECTION

- Not meeting the timeline provided for CAPA
- Not having supporting evidences for CAPAs provided

BDI-Post Inspection for example:

- Not responding to the inspectional findings within the specified time.

- Not having supporting documentary evidences for CAPAs provided

- Not meeting the timeline for implementation of agreed CAPA, not investigated the delay through deviation (*if observed by the agency, a major observation can become critical and may lead to removal of GMP Certificate)*

- Expected to file Interim Report with authorities on implementation of all committed CAPAs

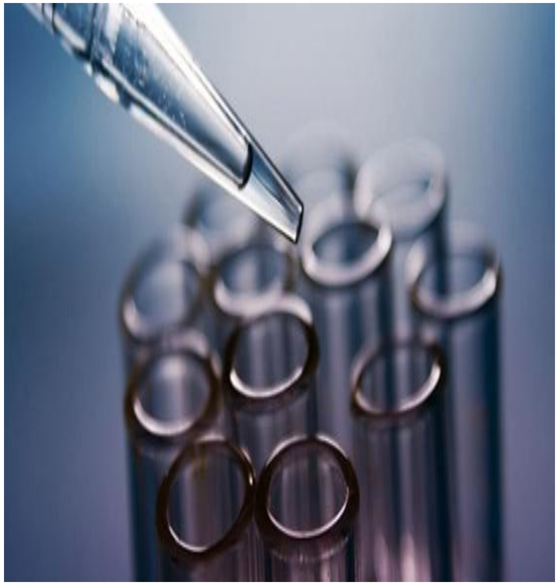
- Any deficiencies leading to BDI identified during Self Inspection shall be reported to GMP inspectorate*.

***Reference: MHRA Web Alert to Industry, Data Governance 16th December, 2013**

Some Causes of Breaches to Data Integrity

Technical (Systems) Aspects

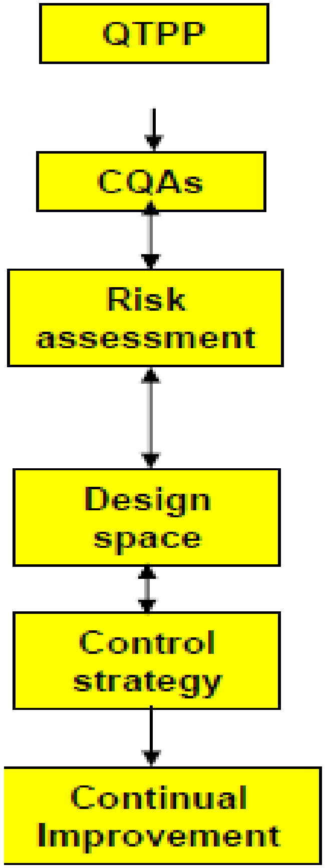
Behavioural Aspects



BDI - CONTRIBUTING FACTORS – TECHNICAL ASPECTS

Product Development & Technology Transfer:

- Unrealistic commitments, inadequate development and associated documentation
- Over commitment regularly contribute to data integrity issues
- Material attributes and Critical Process Parameters – not defined through formal Risk Assessment
- The responsibilities of the technology Sending Unit and Receiving Unit are not defined and / or controlled



VALIDANT
Vital in healthcare

BDI - CONTRIBUTING FACTORS – TECHNICAL ASPECTS

Not following ICH Guidelines
Q8, Q9 & Q10

Overreaching philosophy of quality systems and GMP.

Quality should be built into the product from development through to clinical and subsequent regulatory approval. Testing alone cannot be relied upon to ensure product quality.

In other words, even before commercial manufacture, safety, efficacy and quality of the drug product must be unambiguously established.

VALIDANT
Vital in healthcare

BDI – SOME CONTRIBUTING FACTORS – BEHAVIOURAL

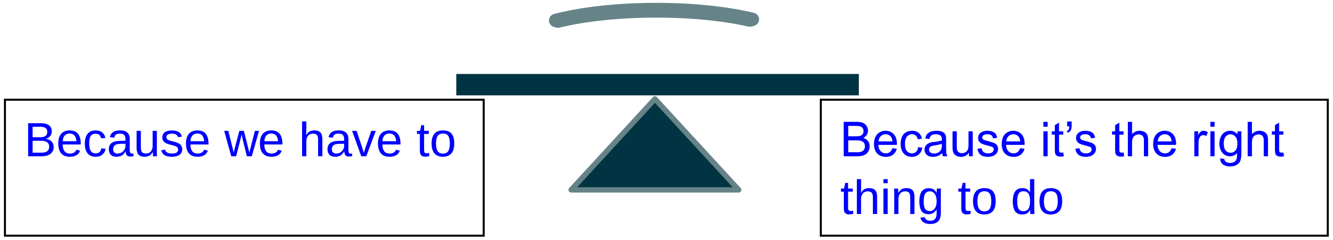
Institutional Bad Habits	Leadership failing to demonstrate the appropriate behaviours. Performance measure that drive the wrong behaviour – focus on short term gains.
Poor Education	Bad decision, inappropriate behaviour. Knowing “How” but not “Why”
Culture of fear and blame	Inability to challenge status-quo.
Poor attitude to problems	Victim mindset vs Learning mindset. Problems are seen as “Bad”
System that Encourages Bad Practices	System complexity and inappropriate design
Hierarchy	Constructive enabling Hierarchy needed
Panic, Stress and Fatigue	Fight, Flight or Freeze
Lack of personnel Integrity and Honesty	“Don’t care” & “I won’t get caught” attitude, have very little pride in what they do,

VALIDANT
Vital in healthcare

Data Integrity

The Way Forward – Culture of Error Management

Tipping Point



Because we have to

Because it's the right thing to do

More of Same?

- ➢Feel embarrassed after making a mistake
- ➢Admission of error – harmful
- ➢Covering up- Why admit when nobody is watching

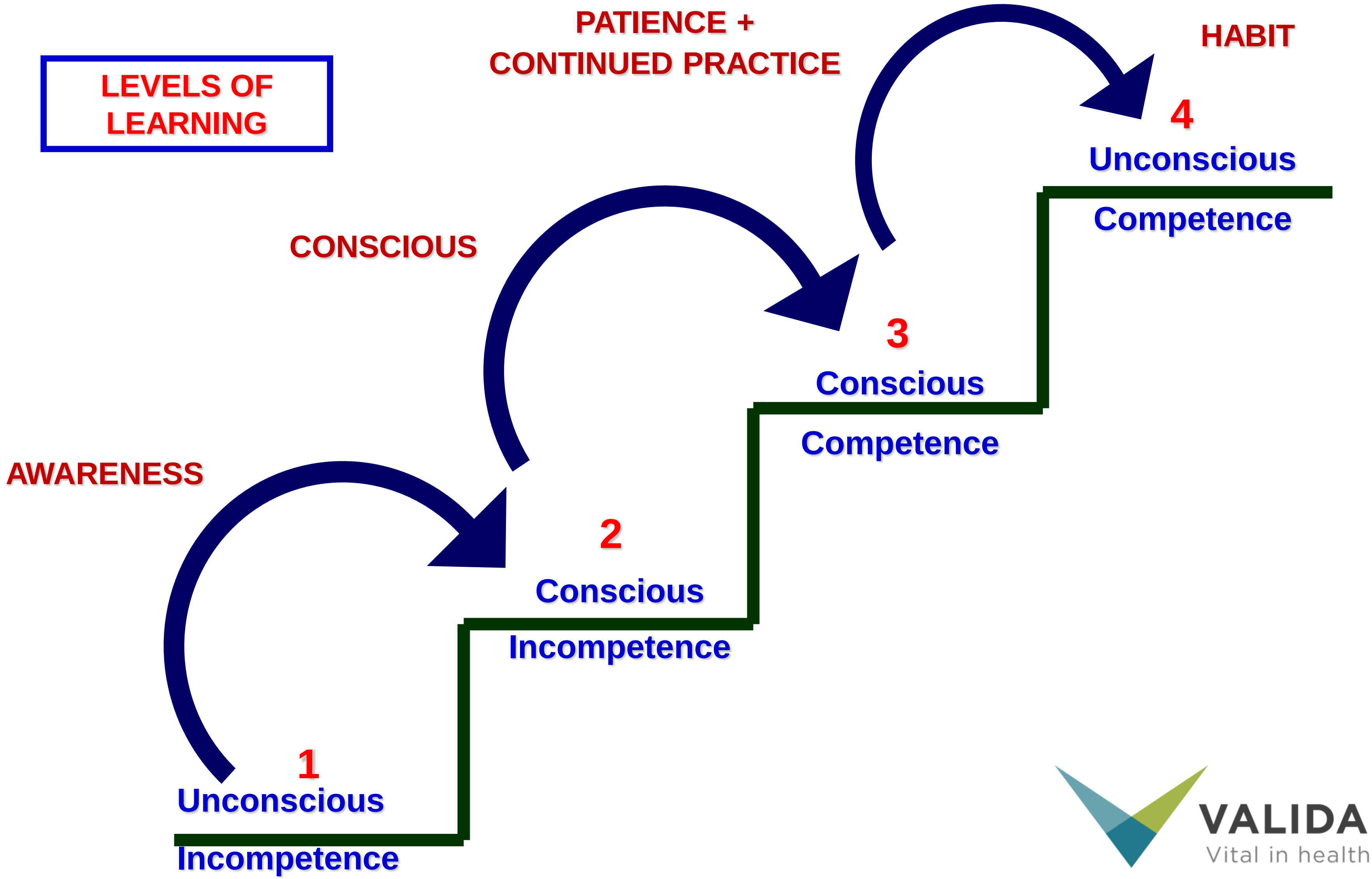
Something Better… Future Focused…

- ➢Put errors to good use
- ➢Share with others
- ➢Analyse and find Root Cause
- ➢Correct errors through QMS
- ➢Anticipate that errors will be made in the learning process
- ➢ Risk acceptance: It needs to be understood that errors may occur

VALIDANT
Vital in healthcare

Data Integrity

SO WHAT NEEDS TO BE DONE?….Achieve the highest level of learning



VALIDANT
Vital in healthcare

Data Integrity

SO WHAT NEEDS TO BE DONE?….Achieve the highest level of learning

- At the highest level of learning- ‘Unconscious Competence’, one is incapable of committing a deliberate error.
- Good Practice becomes second nature
- A good habit is involuntary, needs no supervision, is driven by character ethic and in the face of a challenging situation does not change.

If DI issues are identified

Any deficiencies leading to BDI identified during Self Inspection shall be reported to GMP inspectorate*.

**Reference: MHRA Web Alert to Industry, Data Governance 16th December, 2013*

Wockhardt Warning Letter

Ref. WL: 320-14-01

‘In response to this letter, provide the following to the Agency:

1. A comprehensive evaluation of the extent of the inaccuracy of the reported data.
As part of your comprehensive evaluation, provide a detailed action plan to investigate the extent of the deficient documentation practices noted above;

2. A risk assessment regarding the potential effect on the quality of drug products. As part of your risk assessment, determine the effects of your deficient documentation practices on the quality of the drug product released for distribution; and

3. A management strategy for your firm that includes the details of your global corrective action and preventive action plan.

If DI issues are identified

Wockhardt Warning Letter cntd. (WL 320-14-01)

‘a). As part of your corrective action and preventive action plan, describe the actions you have taken or will take, such as contacting your customers, recalling product, conducting additional testing and/or adding lots to your stability programs to assure stability, monitoring of complaints, or other steps to assure the quality of the product manufactured under the violative conditions discussed above.

b). In addition, as part of your corrective action and preventive action plan, describe the actions you have taken or will take, such as revising procedures, implementing new controls, training or re-training personnel, or other steps to prevent the recurrence of CGMP violations, including breaches of data integrity.’

Data Integrity Presentation References:

Data Integrity, ISPE, Bangalore Chapter Seminar, Creating a Sustainable Quality Culture, 13th December 2014, S.M. Mudda , Executive Director; Technical & Operations, Micro Labs , Bangalore

EudraLex - Volume 4, GMP Guidelines, Annex 11

MHRA GMP Data Integrity Definitions and Guidance for industry 2015.

Catherine Neary (HPRA) Presentation. GMP Information Day 2014.

Data Integrity in FDA Regulated labs, MHRA Data Integrity Requirements, Uday Sheety

WWW.drugregulations.org

MHRA Web Alert to Industry, Data Governance 16th December, 2013

Regulatory Affairs, India's Data Integrity Problems, 3rd February 2015

VALIDANT
Vital in healthcare

AMGEN®

Pioneering science delivers vital medicines™

Data Integrity: A Practical Approach for the QC Laboratory

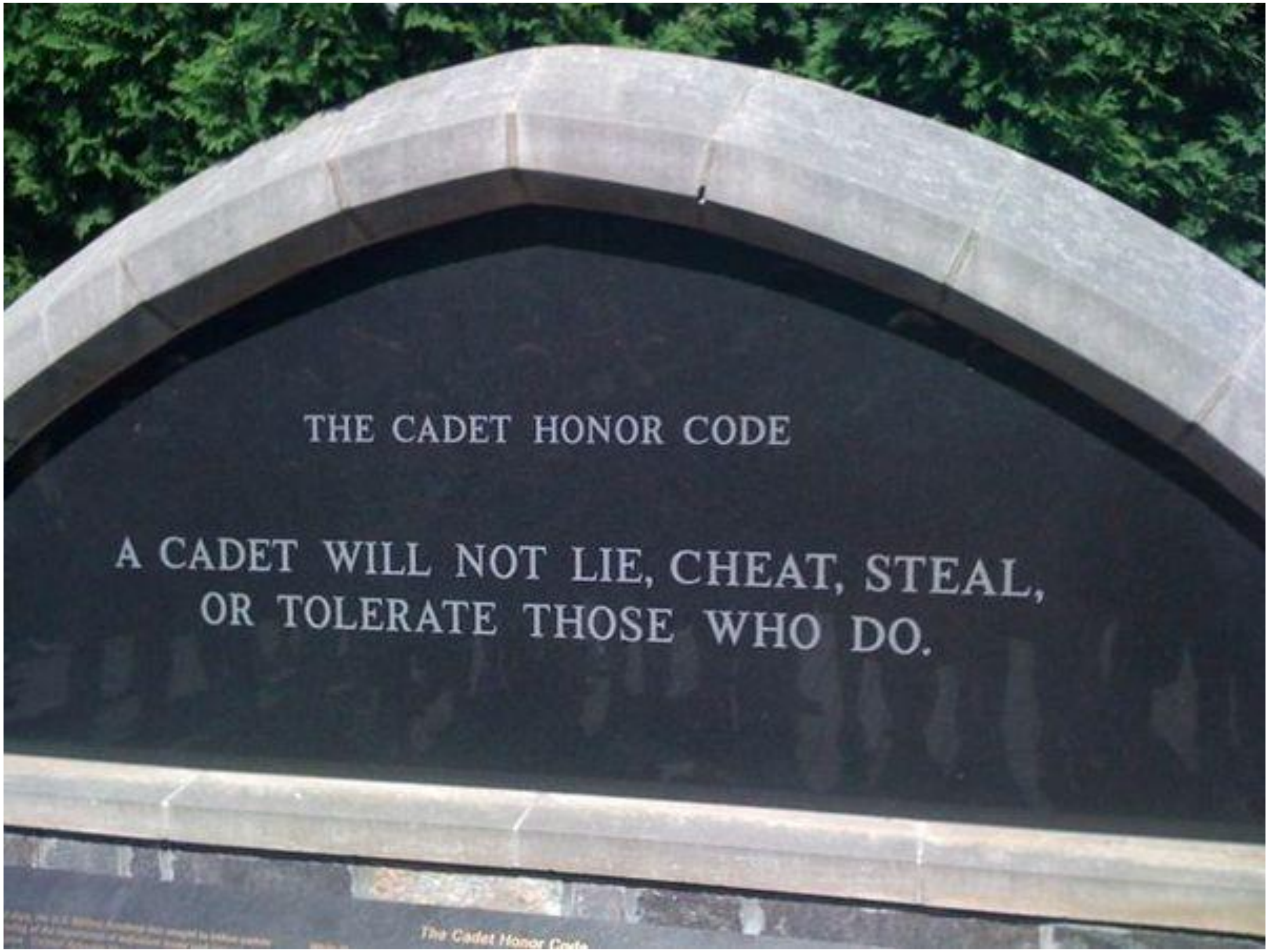
Dan Latham-Timmons – QC Director, Amgen Dun Laoghaire

2015 PDA Data Integrity Seminar

12 May 2015

The Hilton Hotel, Charlemont Place, Dublin 2

US Army Military Academy – West Point


THE CADET HONOR CODE
A CADET WILL NOT LIE, CHEAT, STEAL,
OR TOLERATE THOSE WHO DO.
The Cadet Honor Code

Agenda

- The Laboratory Perspective
- Defining the Objective
- The Most Relevant Predicate Rule
- A little U.S. History
- The Current Reality
- Practical Plan of Action
- Getting the Culture Right
- The Ultimate Future
- Common Examples of Data Integrity Breaches in Industry

The Laboratory Perspective

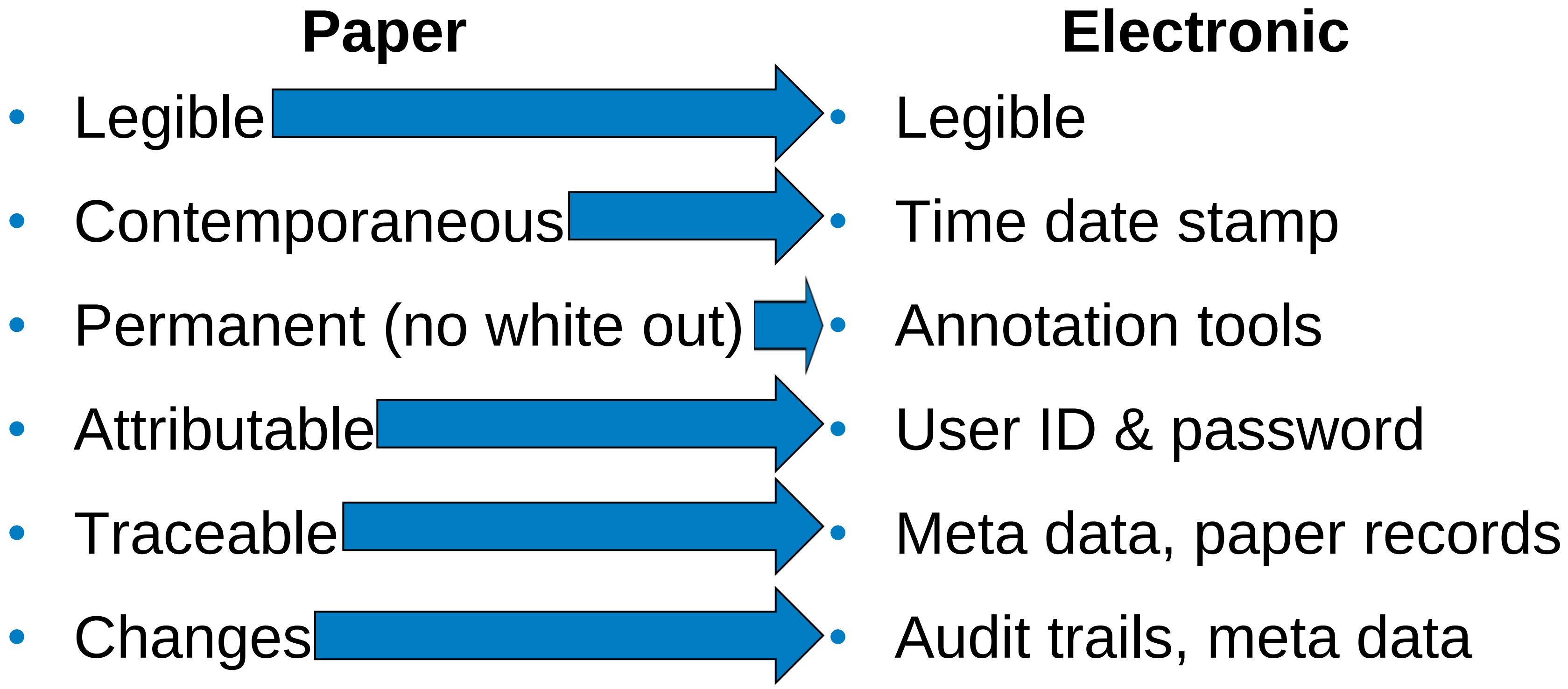
- We are the ultimate guardians of the data.
- We mostly operate with Electronic or Hybrid (electronic + paper) systems.
- We hire “good” people.
- EU and US expectations are aligned.
- True data integrity audits are hard.
- We will need to build on the good culture we already have.

Defining the Objective

- Data Integrity are those elements that give the data its trustworthiness….
- Reliability: Completeness and Accuracy
- Authenticity: It is what it claims to be
- Reviewability: It can be reviewed and interpreted with its full meaning and context

Good Documentation Practices → Trustworthiness

The Most Relevant Predicate Rule



Paper	Electronic
Legible	Legible
Contemporaneous	Time date stamp
Permanent (no white out)	Annotation tools
Attributable	User ID & password
Traceable	Meta data, paper records
Changes	Audit trails, meta data

A Little U.S. History

- Early 1990’s – Industry approaches FDA about electronic submission with electronic signatures
- July 1992 – FDA soliciting comments on electronic signature process
- March 1997 – Issued Part 11 regulation
- 1997-2002 – Industry expressed concern that it would unnecessarily restrict use of technology
- November 2002 – FDA releases guidance document for public comment

A Little More U.S. History

- February 2003 – FDA Withdrew guidance indicating that it may no longer represent their approach under the current good manufacturing practice initiative, and they intend to exercise enforcement discretion with regard to certain Part 11 requirements
- August 2003 – Issued final Guidance for Industry
- 2004 – Pharma Information Systems still are not sure how to comply…seeking clarity
- July 2010- FDA announces Part 11 inspection "in an effort to evaluate industry's compliance and understanding of Part 11“

The Current Reality

- The inspectors have now been trained.
- Data Integrity element of inspections can be variable based on the individual inspectors.
- Rapidly increasing number of data integrity observations.
- Some previous attempts at data integrity have not been completely successful, mostly because of failure to fully consider the human element.
- You already have elements to ensure data integrity, but improvements are required.

Practical Plan of Action

- How do I balance short term and long term action to mitigate risk?
- The phased approach
- Phase one – Immediate risk mitigation
- Phase two – much longer term, but builds robustness for the future

What do I do first?

- Completion of staff awareness training regarding 21CFR Part 11/Annex 11 and electronic GMP documentation controls
- Review of each system's time/date configuration to ensure access to the configuration settings are restricted, preventing system users from modifying the system's time/date
- Ensure accuracy of the system's time/date.
- Review of system roles, through both system configuration and assignment to staff, to ensure appropriate segregation of duties

What do I do first?

- Verification of user appropriateness for each system
- Verification of the existence of procedural controls to perform annual security reviews of user accounts and role assignments
- Review of each system’s configuration to ensure the system forces the user to re login via screen lock or system tools after a period of inactivity
- Update of SOP to incorporate definitions for metadata and audit trails, and the requirements for review of electronic data

What do I do first?

- Completion of the 21 CFR Part 11/Annex 11 Quick Assessment
  - All QC Managers complete the Quick Assessment for the systems in use within their labs and identify remediation activities if necessary
  - QC Managers review the results of each Quick Assessment with the QC Director
  - QC Managers ensure completion of any identified remediation activities

Pop Quiz – Used by Auditors

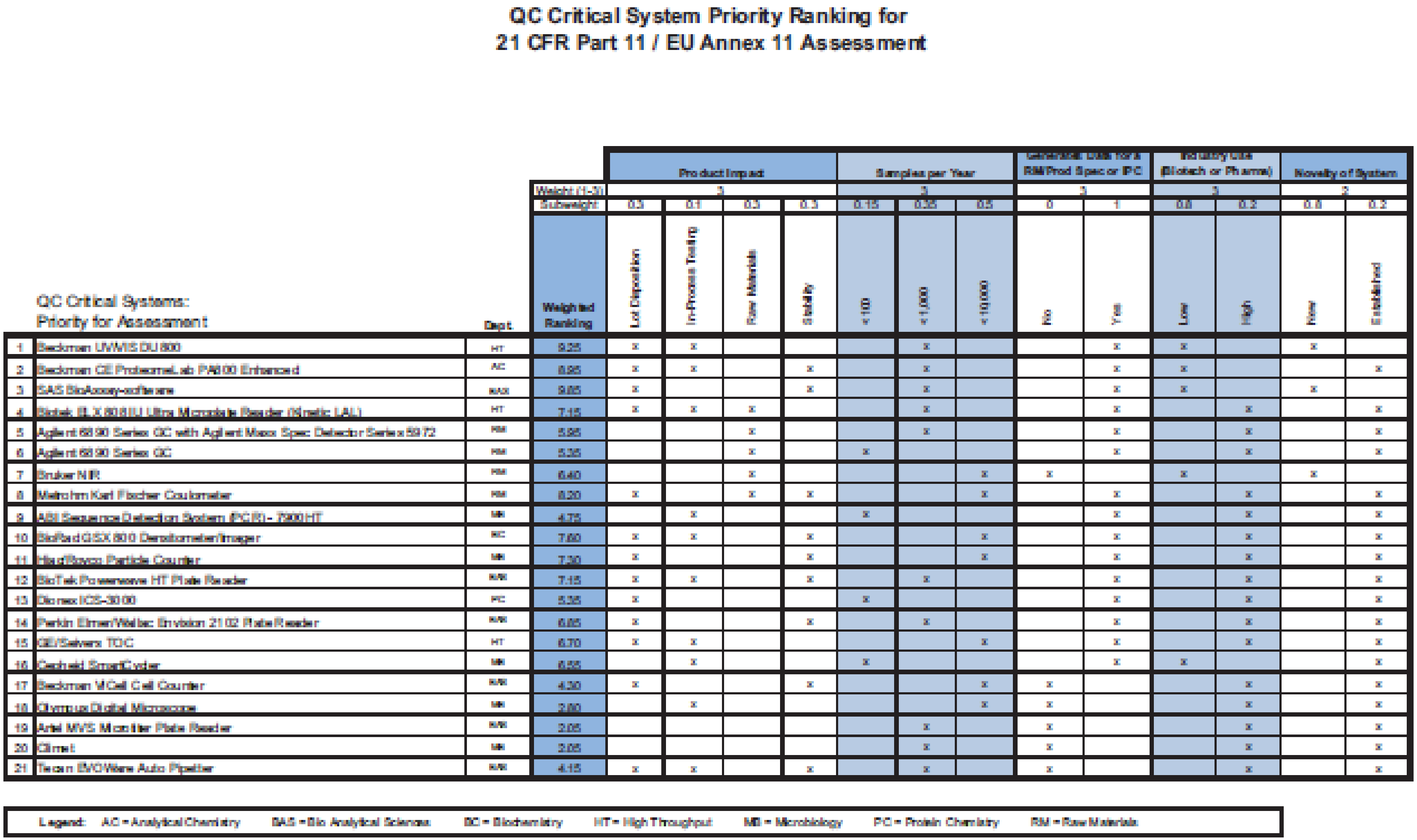
- Do you have your source electronic data (with content & meaning in data Backup & Archive)?
- Do you review your source e-data (or just printouts)?
- Does your review of source e-data include a review of meaningful metadata (such as audit trails or time/date stamps)?
  - SOP's on data review to include review of Audit trail
  - SOP's on data review training – users need to know data flow
- Do you have proper segregation of duties especially regarding system admin/engineer level access.
- Have you validated your system for "intended use" – not just functional testing? (especially important for commercial off the shelf COTS systems)

Prepare your staff – They will be asked these questions

What do you do next – Formal Data Integrity Assessment (DIA)

- Prioritize you're your system by relative risk
  - Product Impact (i.e., used in Lot Disposition, In-Process Testing, Raw Material testing or Stability)
  - Sample results generated per year (i.e., <100, <1000, <10,000)
  - Data usage (i.e., used in Raw Material or Product Specification, or IPC)
  - Industry Use (i.e., typically used in QC Biotech/Pharma industry or not)
  - Novelty of the System (i.e., new or established)
  - Timing for use relative to the current manufacturing schedule
- Order execution of DIA based on relative risk

Example – System Priority Ranking



QC Critical System Priority Ranking for
21 CFR Part 11 / EU Annex 11 Assessment

	QC Critical Systems: Priority for Assessment	Dept.		Product Impact				Samples per Year			Generates Data for a RM/Prod Spec or IPC		Industry Use (Biotech or Pharma)		Novelty of System	
			Weight (1-3)	3				3			3		3		2	
			Subweight	0.3	0.1	0.3	0.3	0.15	0.35	0.5	0	1	0.8	0.2	0.8	0.2
			Weighted Ranking	Lot Disposition	In-Process Testing	Raw Materials	Stability	< 100	< 1,000	< 10,000	No	Yes	Low	High	New	Established
1	Beckman UV/VIS DU 800	HT	9.25	x	x				x			x	x		x	
2	Beckman CE ProteomeLab PA800 Enhanced	AC	8.95	x	x		x		x			x	x			x
3	SAS BioAssay-software	BAS	9.85	x			x		x			x	x		x	
4	Biotek ELX 808IU Ultra Microplate Reader (Kinetic LAL)	HT	7.15	x	x	x			x			x		x		x
5	Agilent 6890 Series GC with Agilent Mass Spec Detector Series 5972	RM	5.95			x			x			x		x		x
6	Agilent 6890 Series GC	RM	5.35			x		x				x		x		x
7	Bruker NIR	RM	6.40			x				x	x		x		x	
8	Metrohm Karl Fischer Coulometer	RM	8.20	x		x	x			x		x		x		x
9	ABI Sequence Detection System (PCR) - 7900HT	MB	4.75		x			x				x		x		x
10	BioRad GSX 800 Densitometer/Imager	BC	7.60	x	x		x			x		x		x		x
11	Hiac/Royco Particle Counter	MB	7.30	x			x			x		x		x		x
12	BioTek Powerwave HT Plate Reader	BAS	7.15	x	x		x		x			x		x		x
13	Dionex ICS-3000	PC	5.35	x				x				x		x		x
14	Perkin Elmer/Wallac Envision 2102 Plate Reader	BAS	6.85	x			x		x			x		x		x
15	GE/Seivers TOC	HT	6.70	x	x					x		x		x		x
16	Cepheid SmartCycler	MB	6.55		x			x				x	x			x
17	Beckman ViCell Cell Counter	BAS	4.30	x			x			x	x			x		x
18	Olympus Digital Microscope	MB	2.80		x					x	x			x		x
19	Ariel MVS Microtiter Plate Reader	BAS	2.05						x		x			x		x
20	Climet	MB	2.05						x		x			x		x
21	Tecan EVOWare Auto Pipetter	BAS	4.15	x	x		x		x		x			x		x

Legend: AC = Analytical Chemistry BAS = Bio Analytical Sciences BC = Biochemistry HT = High Throughput MB = Microbiology PC = Protein Chemistry RM = Raw Materials

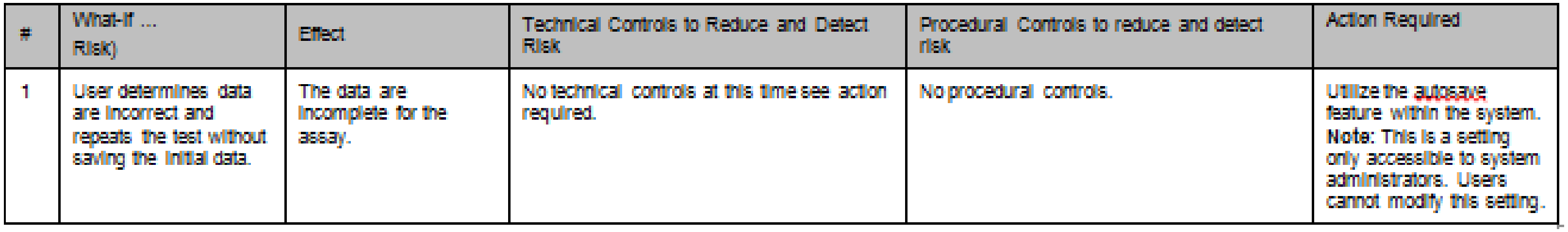
Data Integrity Assessment (DIA)

- The DIA Owner is responsible for selecting a team of SME's to perform the DIA.
- This team will analyse the system to document scenario's that could potentially lead to a data integrity issue.
- The Team will document any 'Findings' and decide on the corrective action
- Analysis with respect to incomplete, inaccurate or missing data. We must ensure all safeguards are in place both technically and procedurally.
    - Data Output / Critical Data Fields / Data Updates / Data Backup & Archive
    - Security – User access and Role Privileges
    - Audit Trail – System Configuration Audit Trail / Data Audit Trail

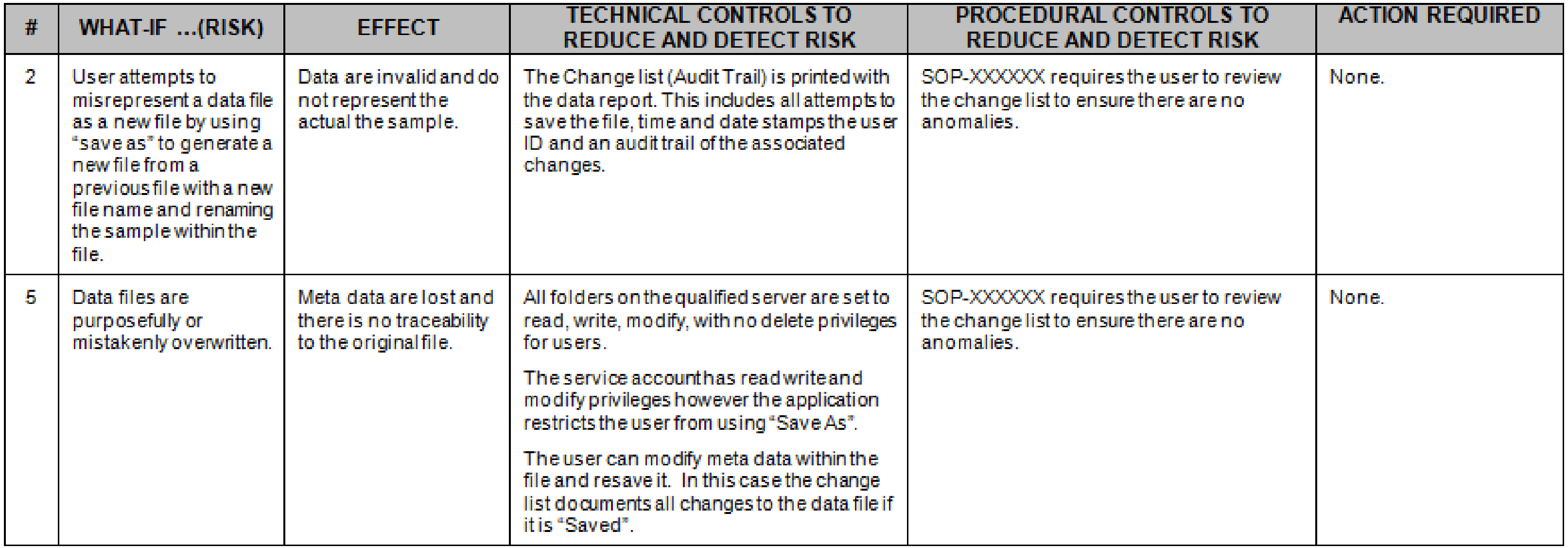
Data Integrity Assessment

- The Team
  - DIA Owner - IS System Owner or Designee
    - Selects the group of SME’s to perform the DIA
    - Calls the Review and Approval meetings
    - Prepares the DIA Summary Report
  - System Owner
    - Participate in analysis of system & review risk items with SME’s to agree if additional controls are required or if risk is acceptable.
    - May be required to perform Pre-Work related to performing DIA (gathering SOP’s / Qualification Documents)
  - Validation
    - Participate in analysis of system, focus on ensuring system is compliant when DIA corrective actions are complete. Purpose is to provide a seamless handover to validation system lifecycle and periodic reviews.
  - QA
    - Participate in analysis of system & review risk items with Business Process owners and System Owners to agree if additional controls are required or if risk is acceptable

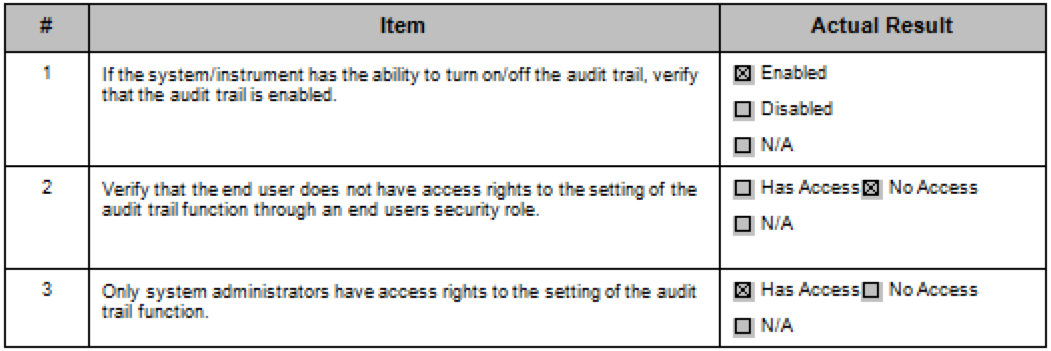
Examples of WHAT-IF (Risk)



#	What-If ... Risk)	Effect	Technical Controls to Reduce and Detect Risk	Procedural Controls to reduce and detect risk	Action Required
1	User determines data are incorrect and repeats the test without saving the initial data.	The data are incomplete for the assay.	No technical controls at this time see action required.	No procedural controls.	Utilize the autosave feature within the system. **Note:** This is a setting only accessible to system administrators. Users cannot modify this setting.



#	WHAT-IF ...(RISK)	EFFECT	TECHNICAL CONTROLS TO REDUCE AND DETECT RISK	PROCEDURAL CONTROLS TO REDUCE AND DETECT RISK	ACTION REQUIRED
2	User attempts to misrepresent a data file as a new file by using "save as" to generate a new file from a previous file with a new file name and renaming the sample within the file.	Data are invalid and do not represent the actual the sample.	The Change list (Audit Trail) is printed with the data report. This includes all attempts to save the file, time and date stamps the user ID and an audit trail of the associated changes.	SOP-XXXXXX requires the user to review the change list to ensure there are no anomalies.	None.
5	Data files are purposefully or mistakenly overwritten.	Meta data are lost and there is no traceability to the original file.	All folders on the qualified server are set to read, write, modify, with no delete privileges for users. The service account has read write and modify privileges however the application restricts the user from using "Save As". The user can modify meta data within the file and resave it. In this case the change list documents all changes to the data file if it is "Saved".	SOP-XXXXXX requires the user to review the change list to ensure there are no anomalies.	None.



#	Item	Actual Result
1	If the system/instrument has the ability to turn on/off the audit trail, verify that the audit trail is enabled.	☒ Enabled □ Disabled □ N/A
2	Verify that the end user does not have access rights to the setting of the audit trail function through an end users security role.	□ Has Access ☒ No Access □ N/A
3	Only system administrators have access rights to the setting of the audit trail function.	☒ Has Access □ No Access □ N/A

Getting the Culture Right

- People who get paid to think for a living need to have a clear understanding of why before they can fully engage.
  - Give them the context, then give it to them again and again…
- Make the most responsible person (i.e., QC Director) give the training and answer the hard questions
- People learn one of 3 way… by example, by example and by example. Provide them with an example rich environment
- Law of unintended consequences – how management can get it wrong

Have a Plan Before You Find Aberrant Data

- Partner with HR, legal and QA
- Determine how to document in the Quality Management Tracking System
- For HR investigations privacy is critical
- What action is appropriate for what infraction
  - Verbal warning
  - Written Warning
  - Demotion
  - Termination
- How much previous data will you need to review?

The Ultimate Future

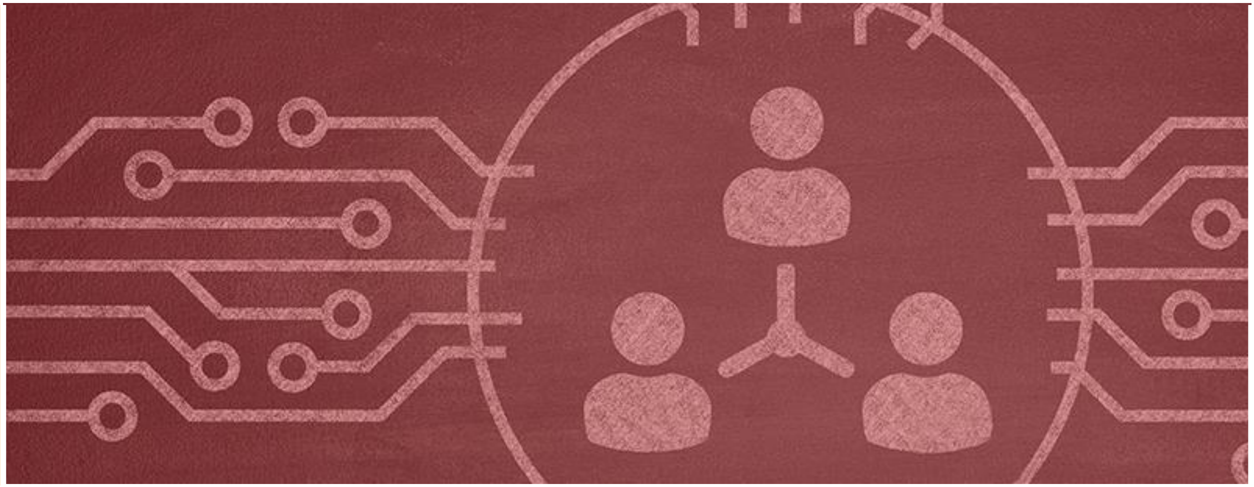
- Fully integrated electronic system
- Laboratory Method Execution System (LMES, electronic notebook)
- Consumable Inventory Management System (CIMS)
- Laboratory Information Management System (LIMS)
- Asset Management System (e.g., Maximo)
- LMES+CIMS+LIMS+Maximo=Integrated Solution

Even fully integrated systems require staff training and the review of some metadata

Common Examples of Data Integrity Breaches in Industry

- Lab staff given administrator access to gain access to audit trail
  - Delete data
  - Change clock
- Annotation available and not audit trailed
- Not reviewing metadata or audit trail – limiting context.
- Reviewing paper instead of electronic source
- Using uncontrolled forms attached to SOP’s
- Sharing passwords due to system limitations
- Leaving an open computer unattended

Thank You



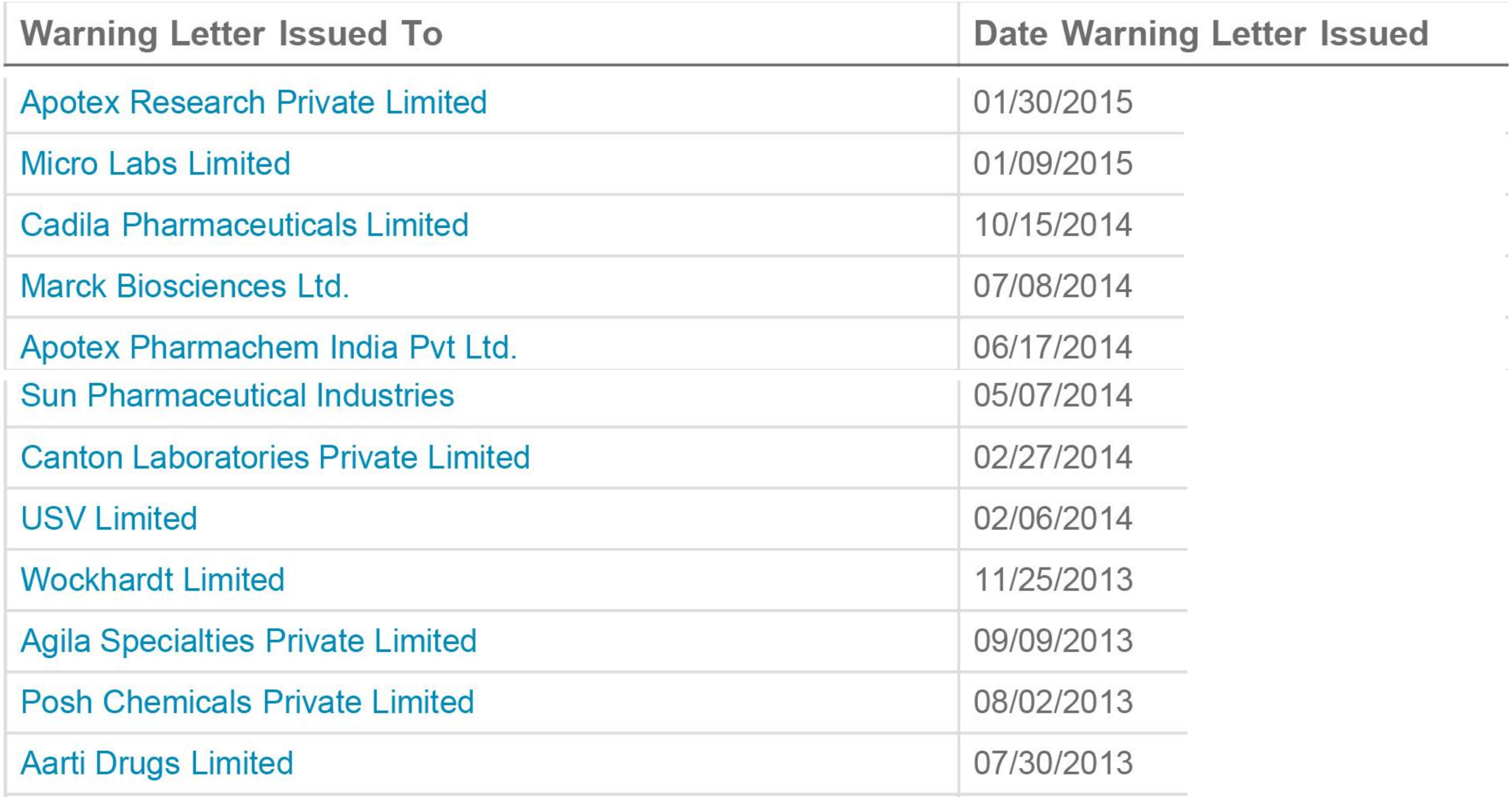
Focus on Patient and Product Quality as the foundation for Data Integrity

Madlene Dole, Head Strategic Planning and Operations – Novartis Group Quality

May 12, 2015

NOVARTIS

FDA Warning Letters about DI to Indian suppliers



Warning Letter Issued To	Date Warning Letter Issued
Apotex Research Private Limited	01/30/2015
Micro Labs Limited	01/09/2015
Cadila Pharmaceuticals Limited	10/15/2014
Marck Biosciences Ltd.	07/08/2014
Apotex Pharmachem India Pvt Ltd.	06/17/2014
Sun Pharmaceutical Industries	05/07/2014
Canton Laboratories Private Limited	02/27/2014
USV Limited	02/06/2014
Wockhardt Limited	11/25/2013
Agila Specialties Private Limited	09/09/2013
Posh Chemicals Private Limited	08/02/2013
Aarti Drugs Limited	07/30/2013

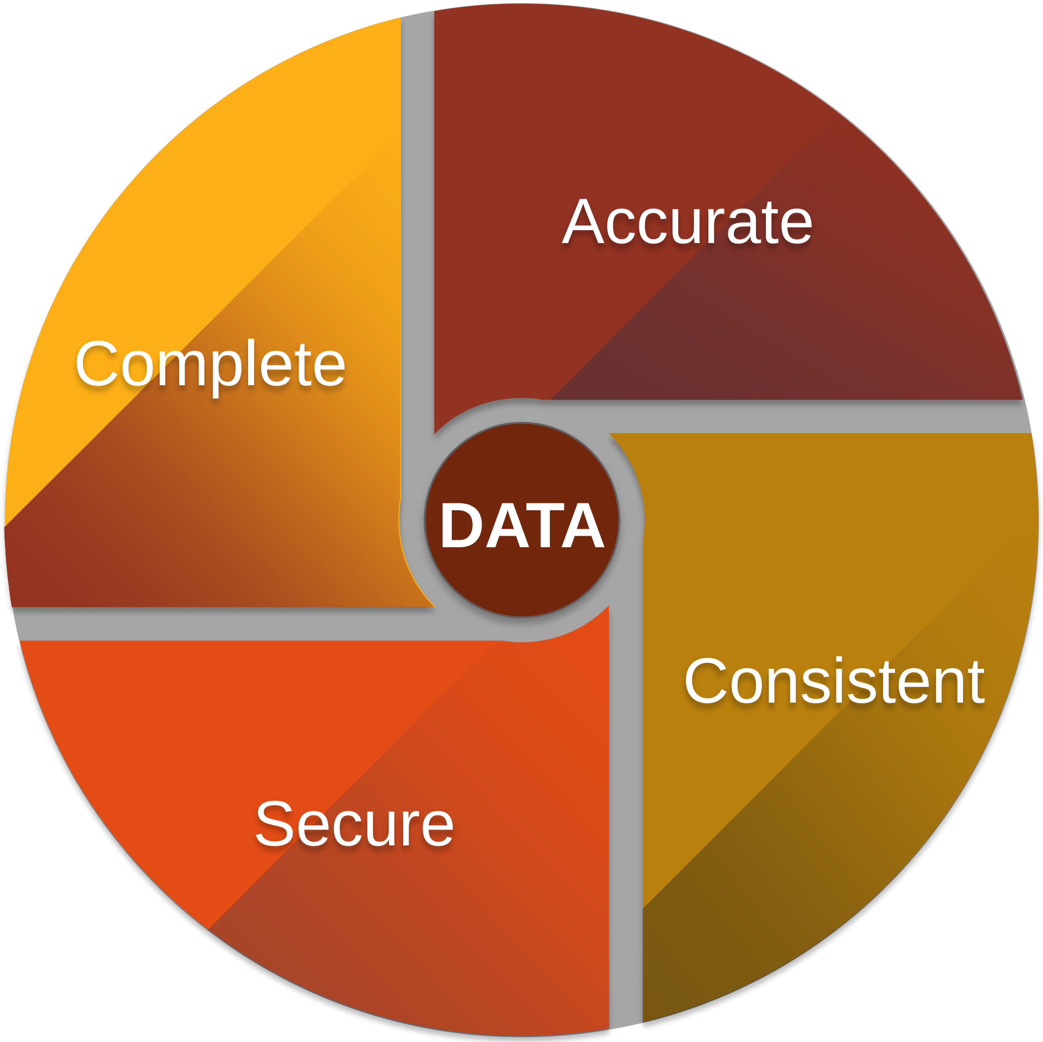
EU regulators are taking strong action on DI

EMA Recommends Suspending Drugs over GVK Data Integrity Issues

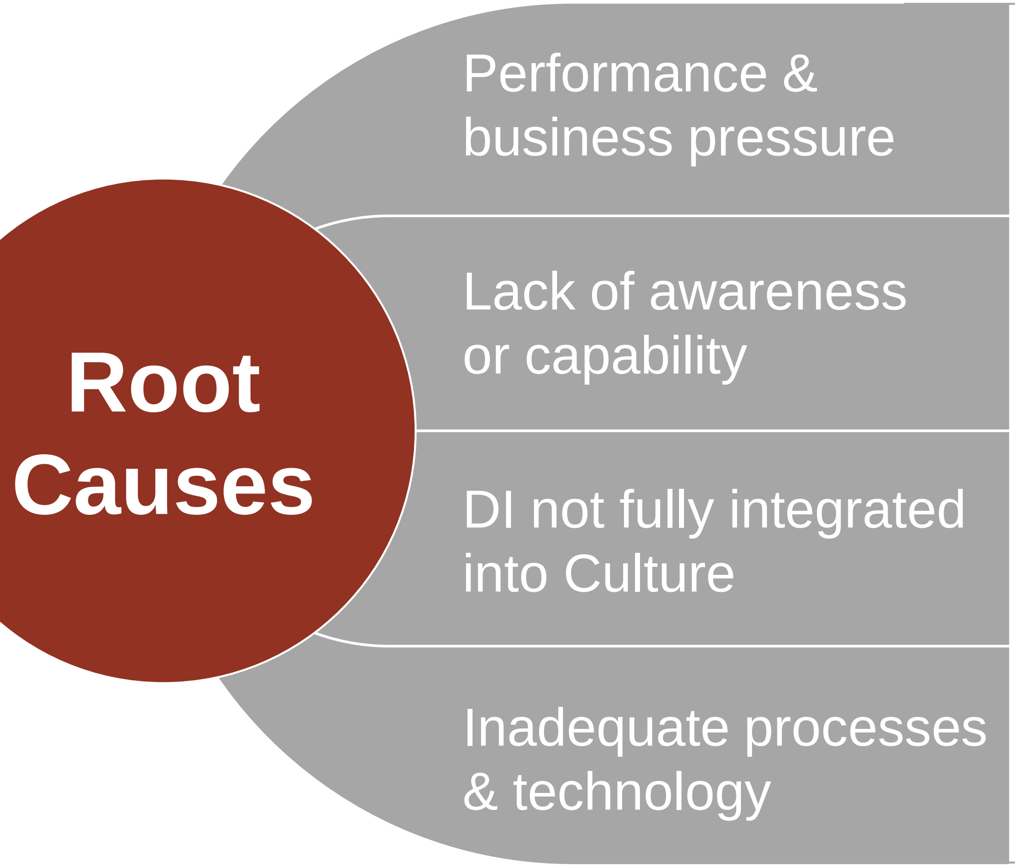
Posted 23 January 2015

More than 700 Products Recommended for Suspension

Data Integrity: what are we aiming for?



Why is it so hard for companies to get it right?!



Root Causes

Performance & business pressure

Lack of awareness or capability

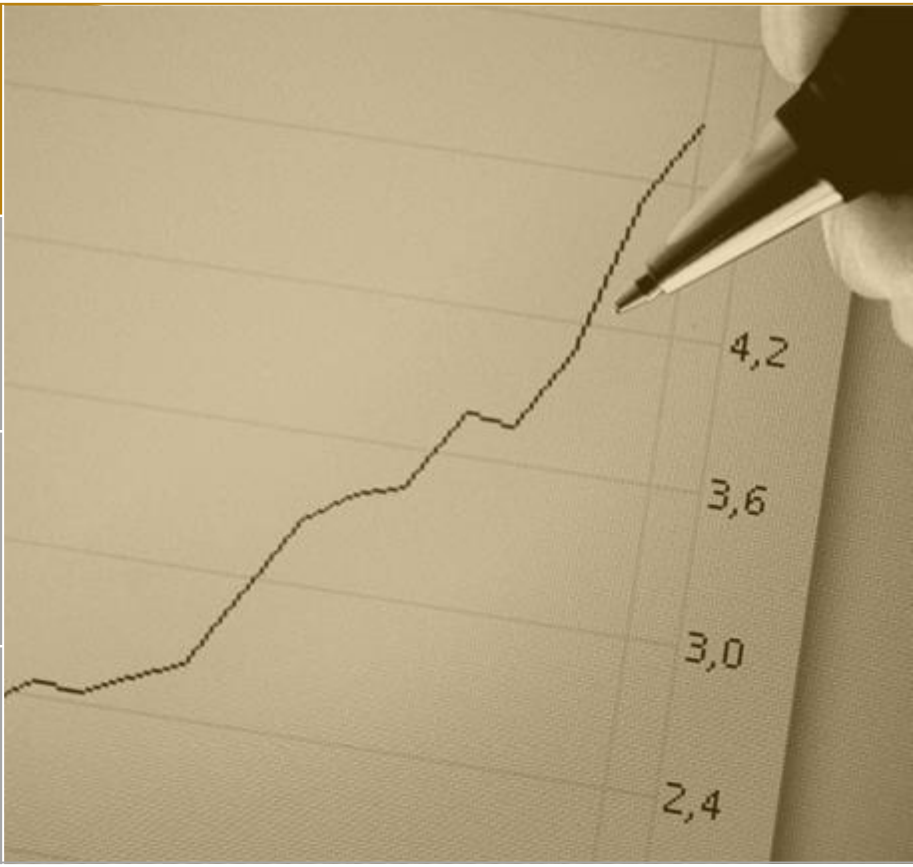
DI not fully integrated into Culture

Inadequate processes & technology

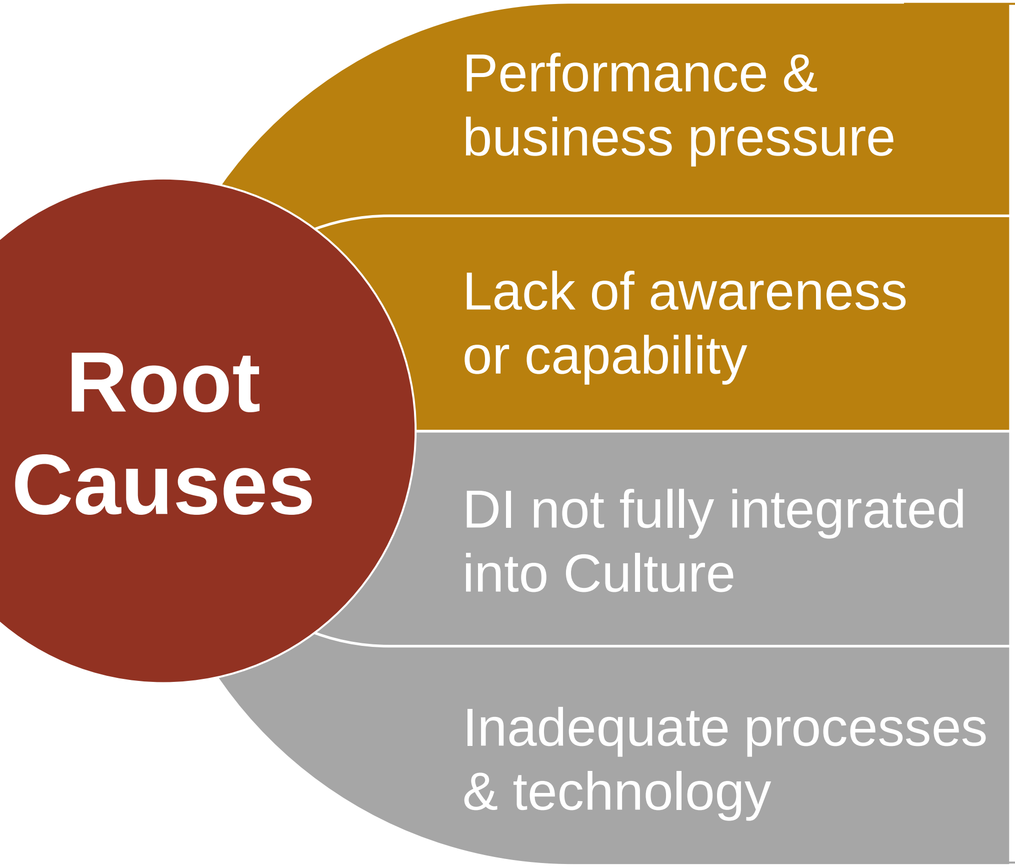
Why is it so hard for companies to get it right?!

Root Causes

- Performance & business pressure
- Lack of awareness or capability
- DI not fully integrated into Culture
- Inadequate processes & technology



Why is it so hard for companies to get it right?!



Root Causes

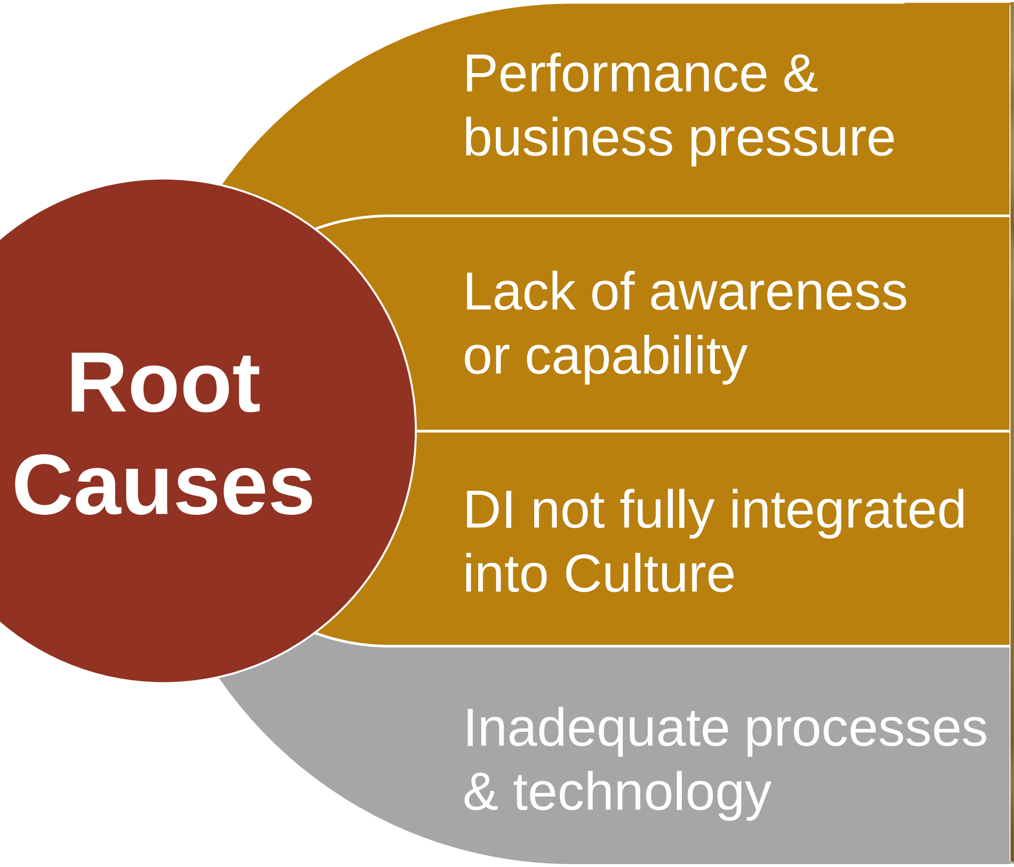
Performance & business pressure

Lack of awareness or capability

DI not fully integrated into Culture

Inadequate processes & technology

Why is it so hard for companies to get it right?!



Root Causes

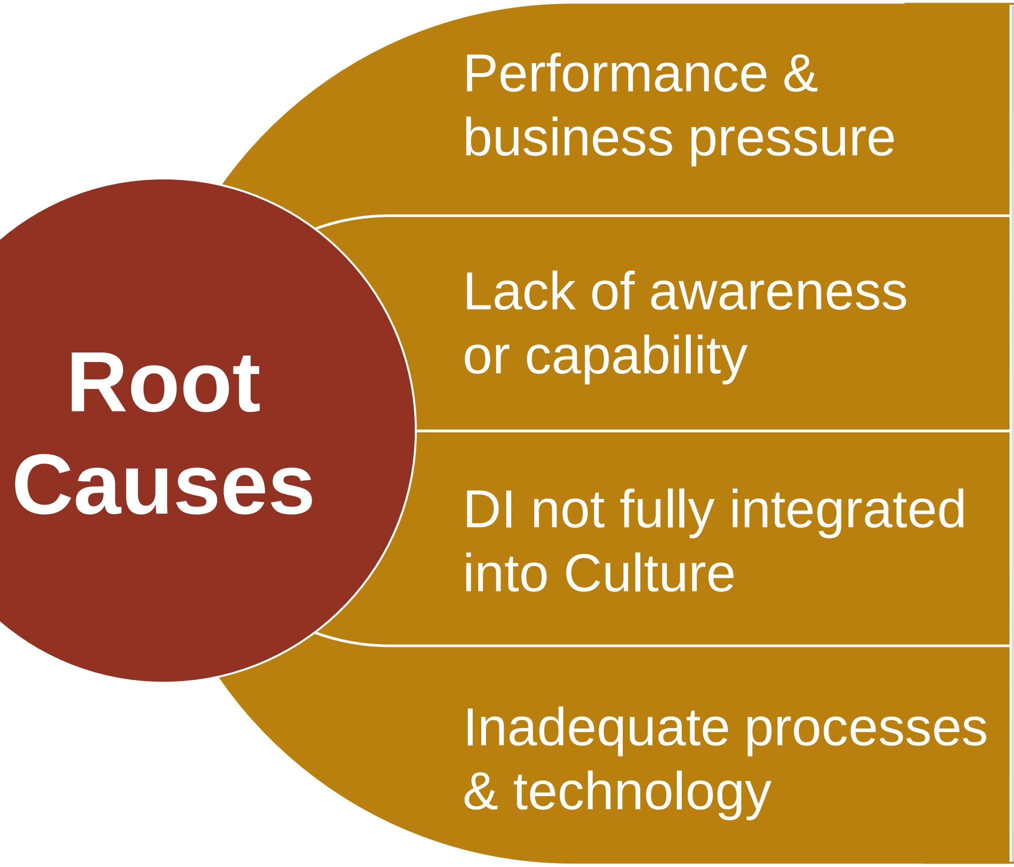
Performance & business pressure

Lack of awareness or capability

DI not fully integrated into Culture

Inadequate processes & technology

Why is it so hard for companies to get it right?!



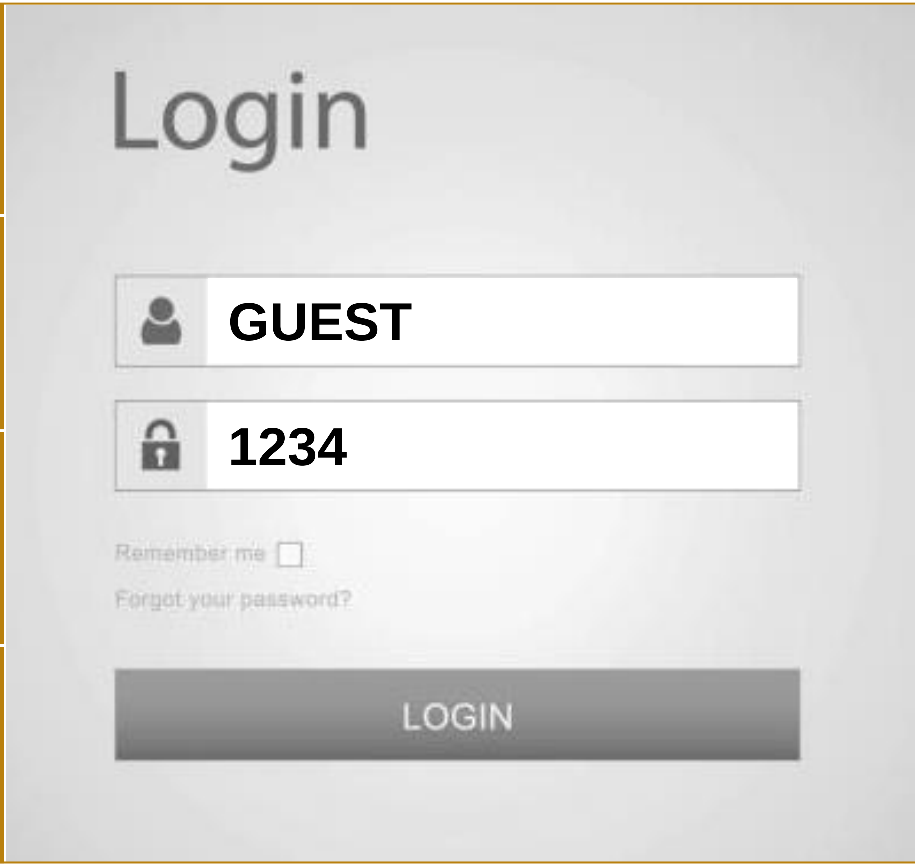
Root Causes

Performance & business pressure

Lack of awareness or capability

DI not fully integrated into Culture

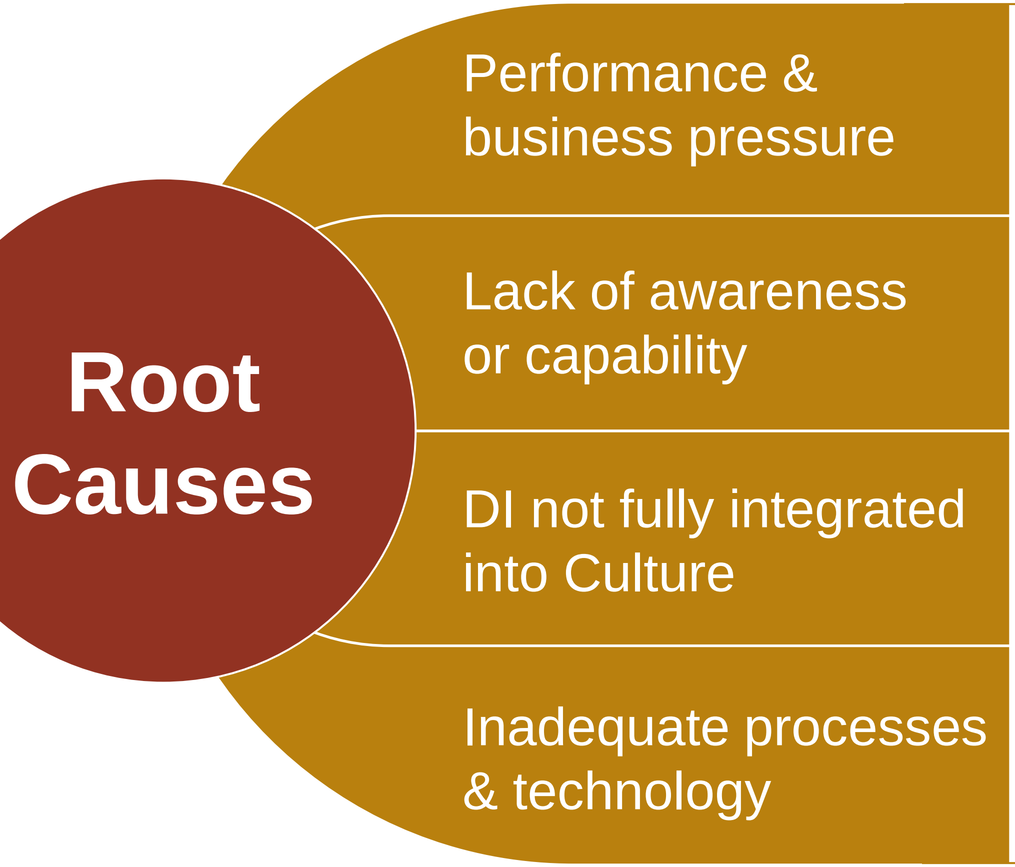
Inadequate processes & technology



GUEST

1234

Why is it so hard for companies to get it right?!



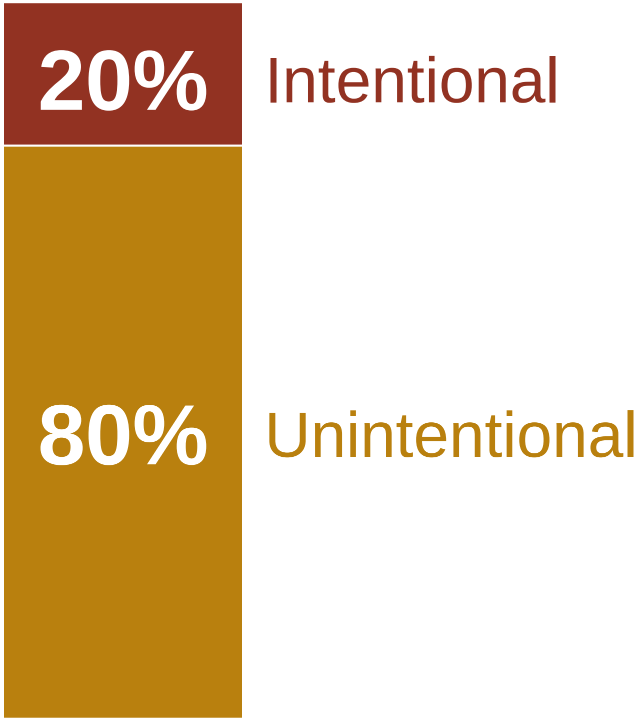
Root Causes

Performance & business pressure

Lack of awareness or capability

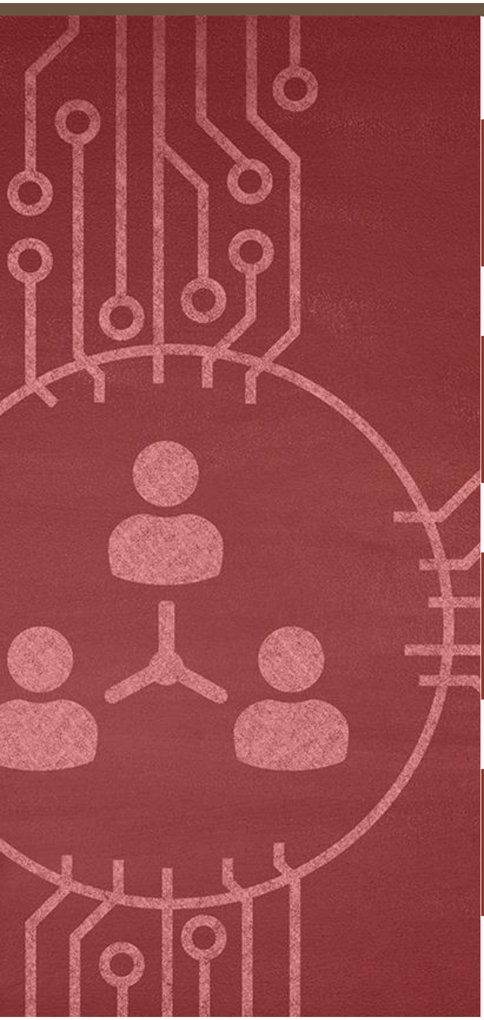
DI not fully integrated into Culture

Inadequate processes & technology



Sources: Novartis V&D analysis 2014; Monica Cahilly

Four vital steps towards Data Integrity



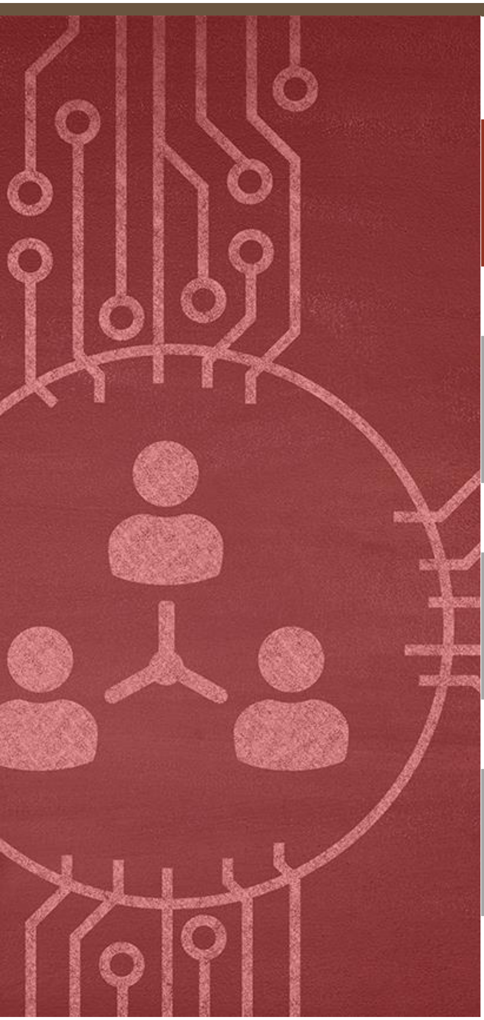
1 Education and Communication

2 Detection and Mitigation of Risks

3 Technology and IT Systems

4 Governance of DI

Four vital steps towards Data Integrity



1. Education and Communication
2. Detection and Mitigation of Risks
3. Technology and IT Systems
4. Governance of DI

What education? What communication?

How to recognize DI issues

EDUCATE

DI is *everyone's* responsibility

COMMUNICATE

Examples of how we’re communicating the risks

....and related impact!

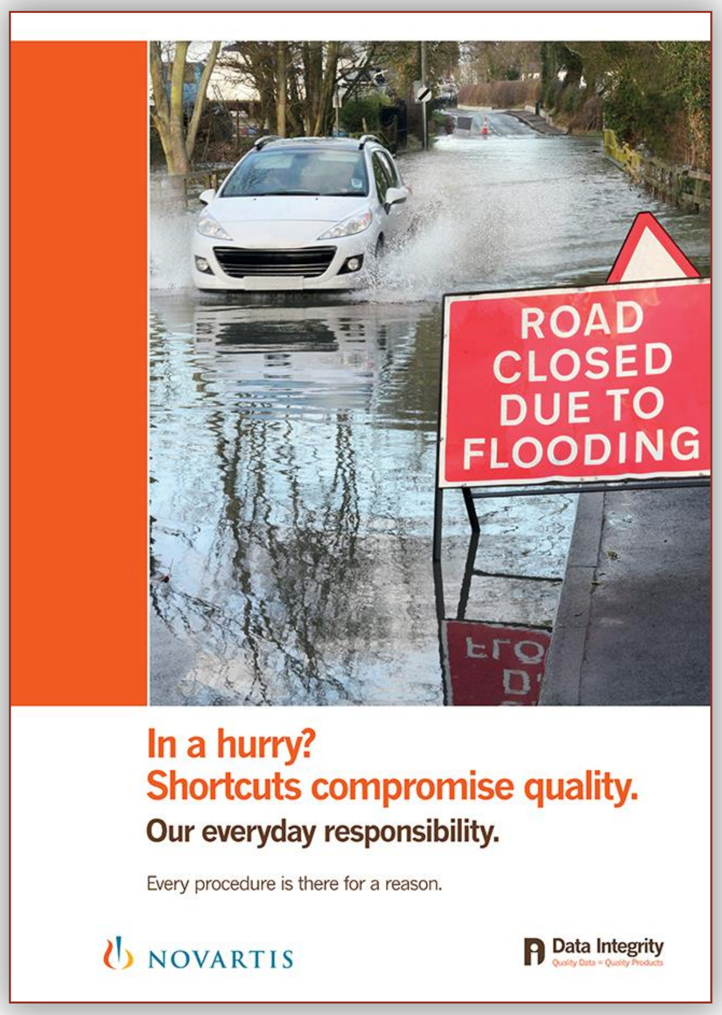
Without data, we don’t have a product.

Our everyday responsibility.

Without a product we can’t supply our patients.

NOVARTIS

Data Integrity
Quality Data = Quality Products



In a hurry?
Shortcuts compromise quality.

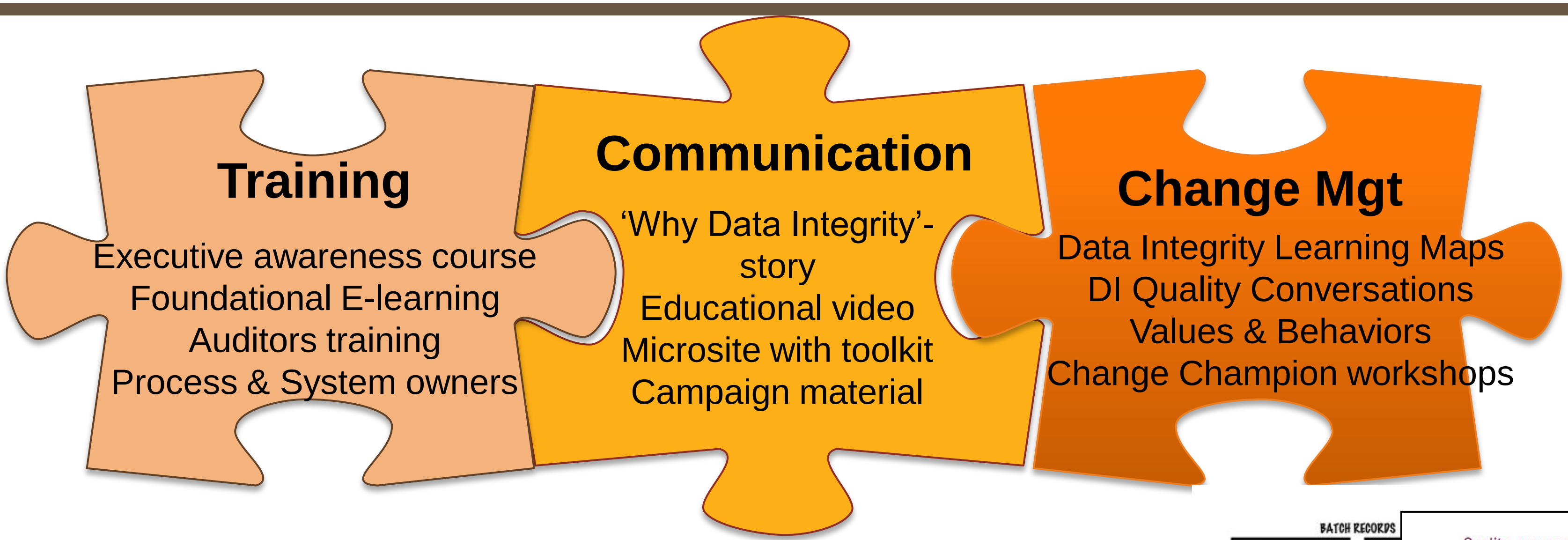
Our everyday responsibility.

Every procedure is there for a reason.

NOVARTIS

Data Integrity
Quality Data = Quality Products

Culture and education is the foundation for a strong Data Integrity mindset



Training

Executive awareness course
Foundational E-learning
Auditors training
Process & System owners

Communication

'Why Data Integrity'-story
Educational video
Microsite with toolkit
Campaign material

Change Mgt

Data Integrity Learning Maps
DI Quality Conversations
Values & Behaviors
Change Champion workshops

NOVARTIS

GxP TRAINING

Data Integrity Foundational Training

Data Integrity, the Data Lifecycle, and GDP for All GxP Audiences

NOVARTIS

Executive Management Training 2014

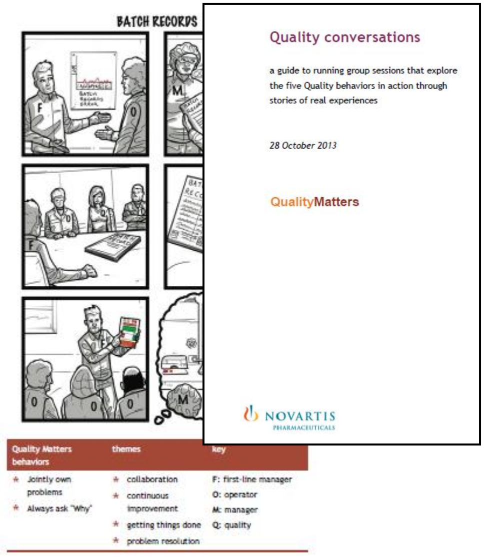
Data Integrity eLearning

Course Outline

Course Aim

Data Integrity Definitions
ALCOA Leaflet

Data Integrity microsite



Quality conversations

a guide to running group sessions that explore the five Quality behaviors in action through stories of real experiences

28 October 2013

QualityMatters

NOVARTIS PHARMACEUTICALS

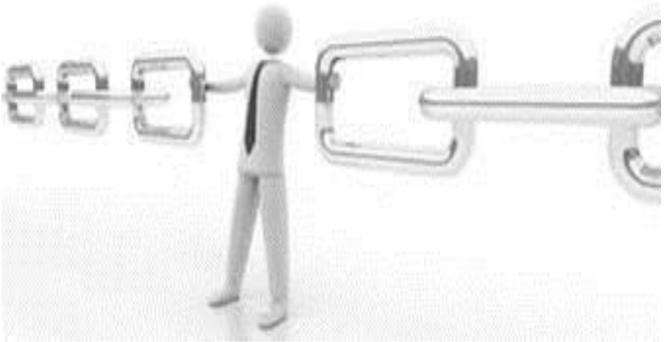
Quality Matters behaviors	themes	key
★ Jointly own problems ★ Always ask "Why"	★ collaboration ★ continuous improvement ★ getting things done ★ problem resolution	F: first-line manager O: operator M: manager Q: quality

People are always an element of control.....

....so **mindset shift** to strengthen understanding of Data Integrity and impact on patients safety and product quality are key.

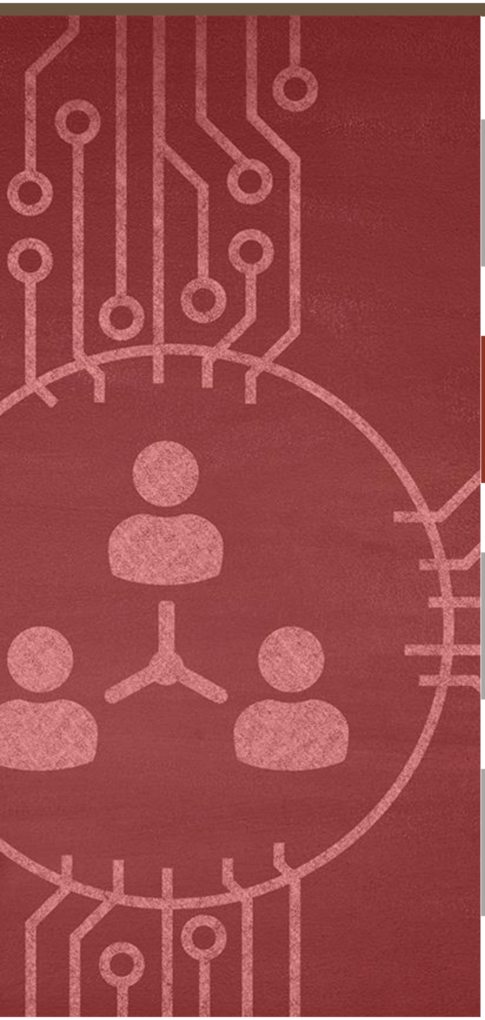
Education and consistent communication ensure:

- A common understanding
- Awareness of impact
- Ownership
- Leadership support



Any further activities can now build on this to ensure sustainability!

Four vital steps towards Data Integrity



1 Education and Communication

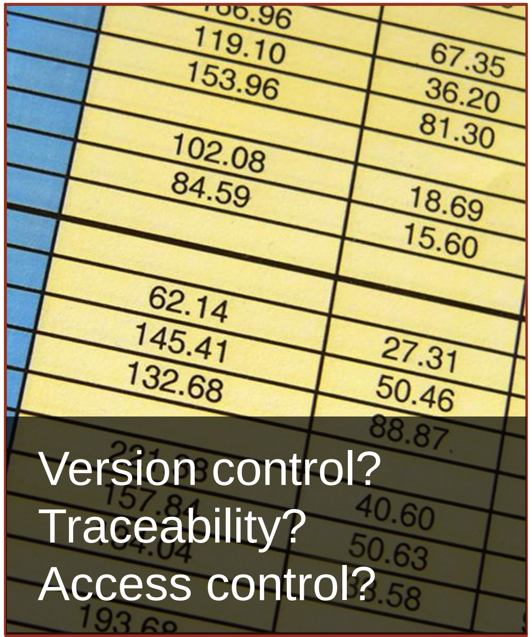
2 Detection and Mitigation of Risks

3 Technology and IT Systems

4 Governance of DI

Understand risks: known risk areas

Understand current risks



Version control?
Traceability?
Access control?

SPREADSHEETS

Archiving raw data?
Audit trail?
Segregation of duty?

STAND-ALONE

Access control?
Accountability?
Traceability?

INSECURE ID

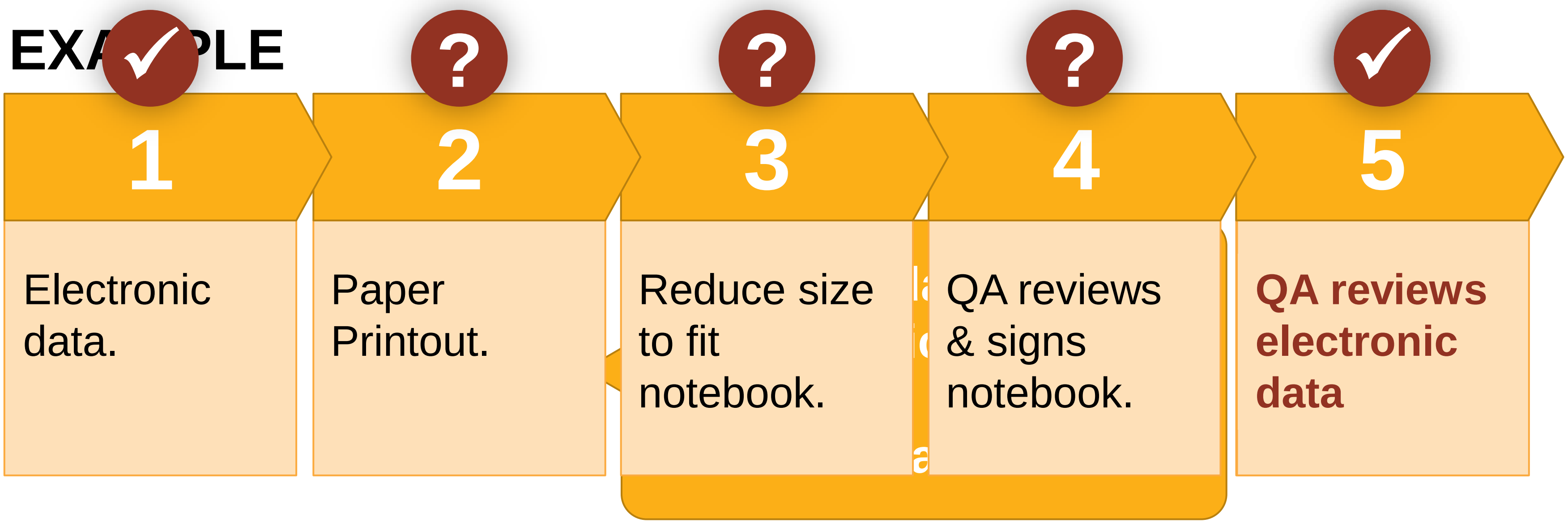
NOVARTIS

DLCPM*: understand risks, optimize processes

**Data Lifecycle Process Mapping*

Mitigate risks

EXAMPLE



✓ **1** Electronic data.

? **2** Paper Printout.

? **3** Reduce size to fit notebook.

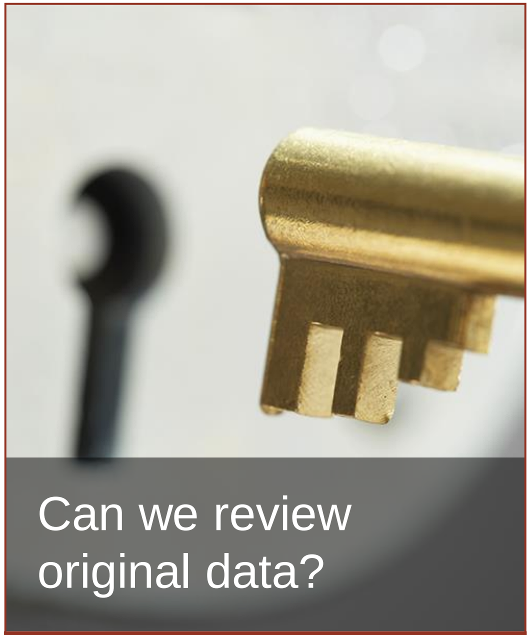
? **4** QA reviews & signs notebook.

✓ **5** **QA reviews electronic data**

Understand risks through DLCPM*

**Data Lifecycle Process Mapping*

Mitigate risks

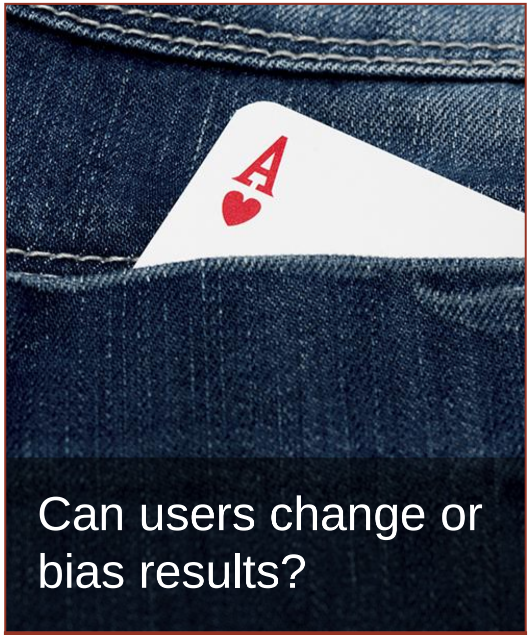


Can we review original data?

AVAILABILITY

Do users (not just IT) understand data flow?

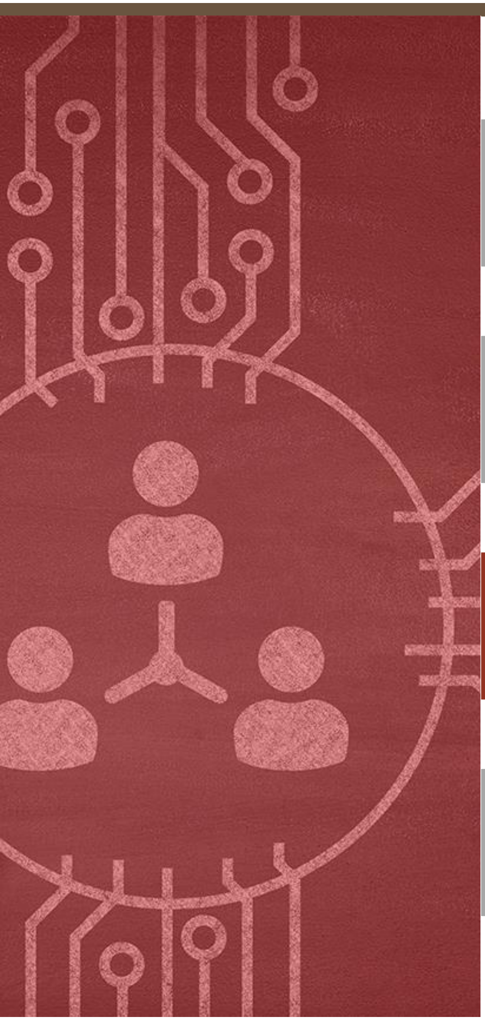
OWNERSHIP



Can users change or bias results?

CONTROLS

Four vital steps towards Data Integrity



1 Education and Communication

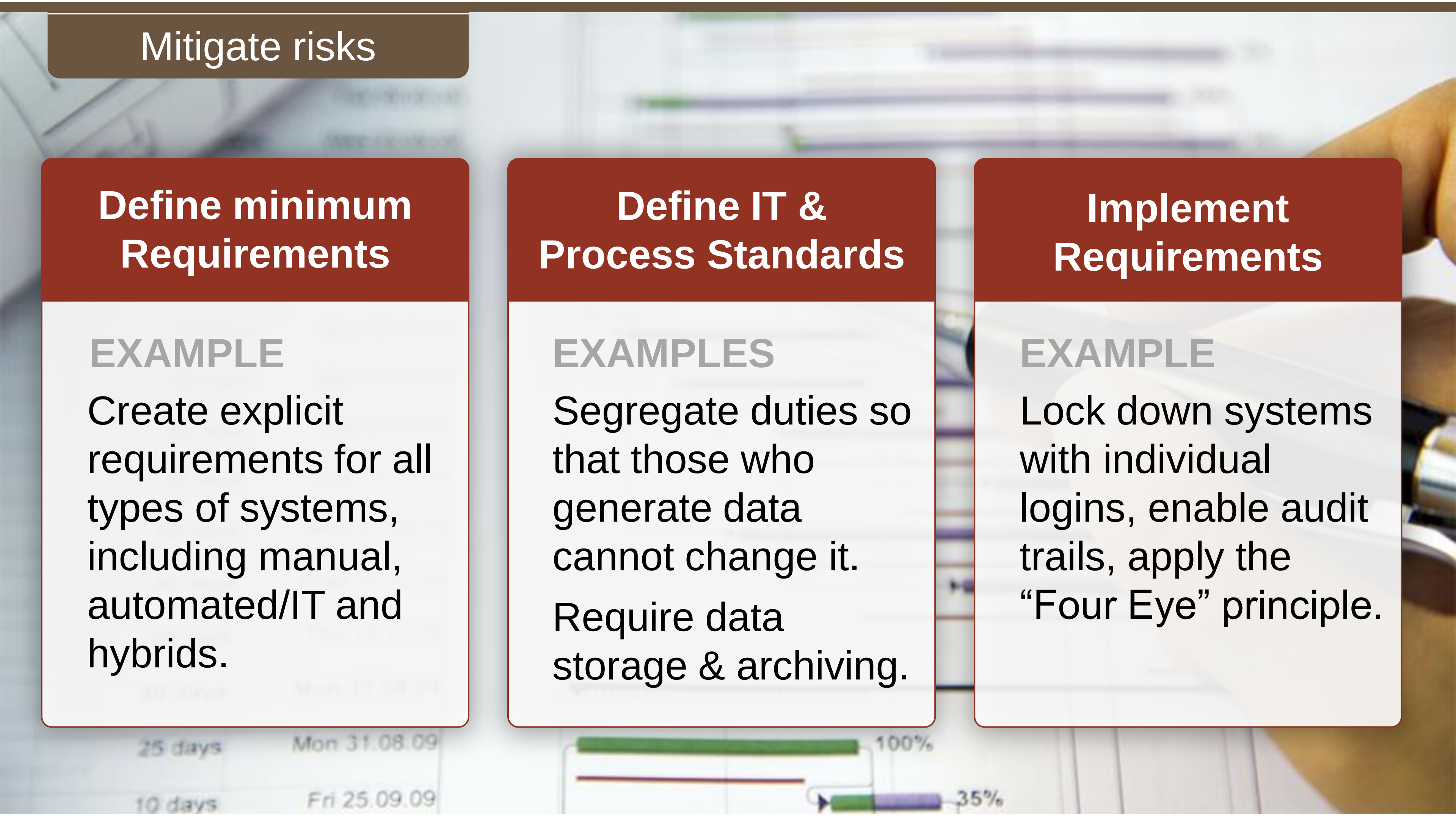
2 Detection and Mitigation of Risks

3 Technology and IT Systems

4 Governance of DI

NOVARTIS

Processes & systems: prevent risks from emerging



Mitigate risks

Define minimum Requirements

EXAMPLE

Create explicit requirements for all types of systems, including manual, automated/IT and hybrids.

Define IT & Process Standards

EXAMPLES

Segregate duties so that those who generate data cannot change it.

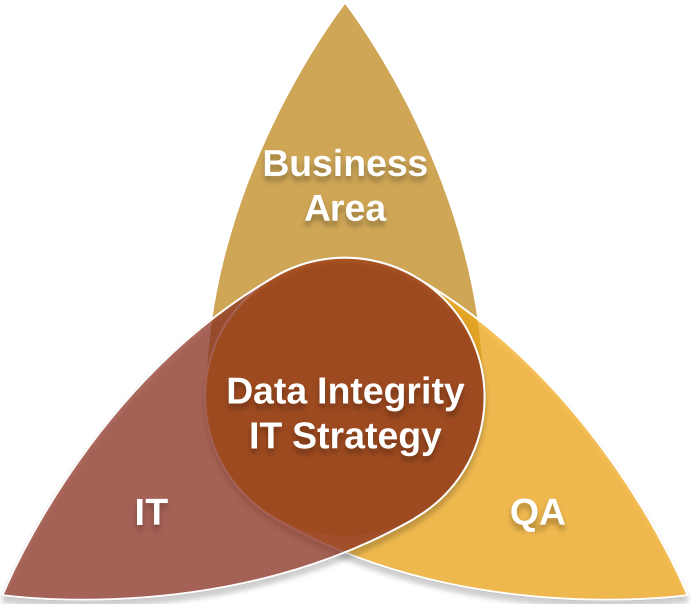
Require data storage & archiving.

Implement Requirements

EXAMPLE

Lock down systems with individual logins, enable audit trails, apply the “Four Eye” principle.

Define IT and technology strategy

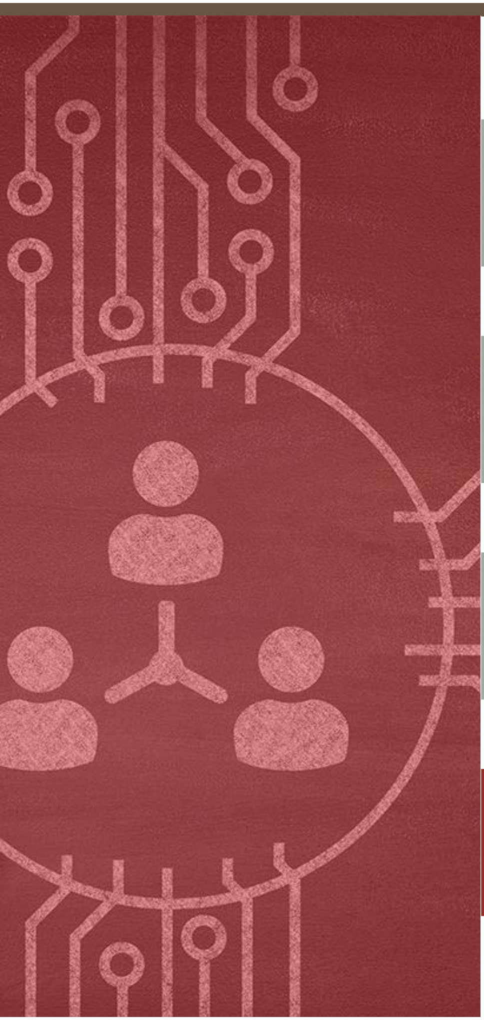


What does our technology landscape vision look like?

How far and fast do we want to move towards our vision?

What are our options? What's practical?

Four vital steps towards Data Integrity



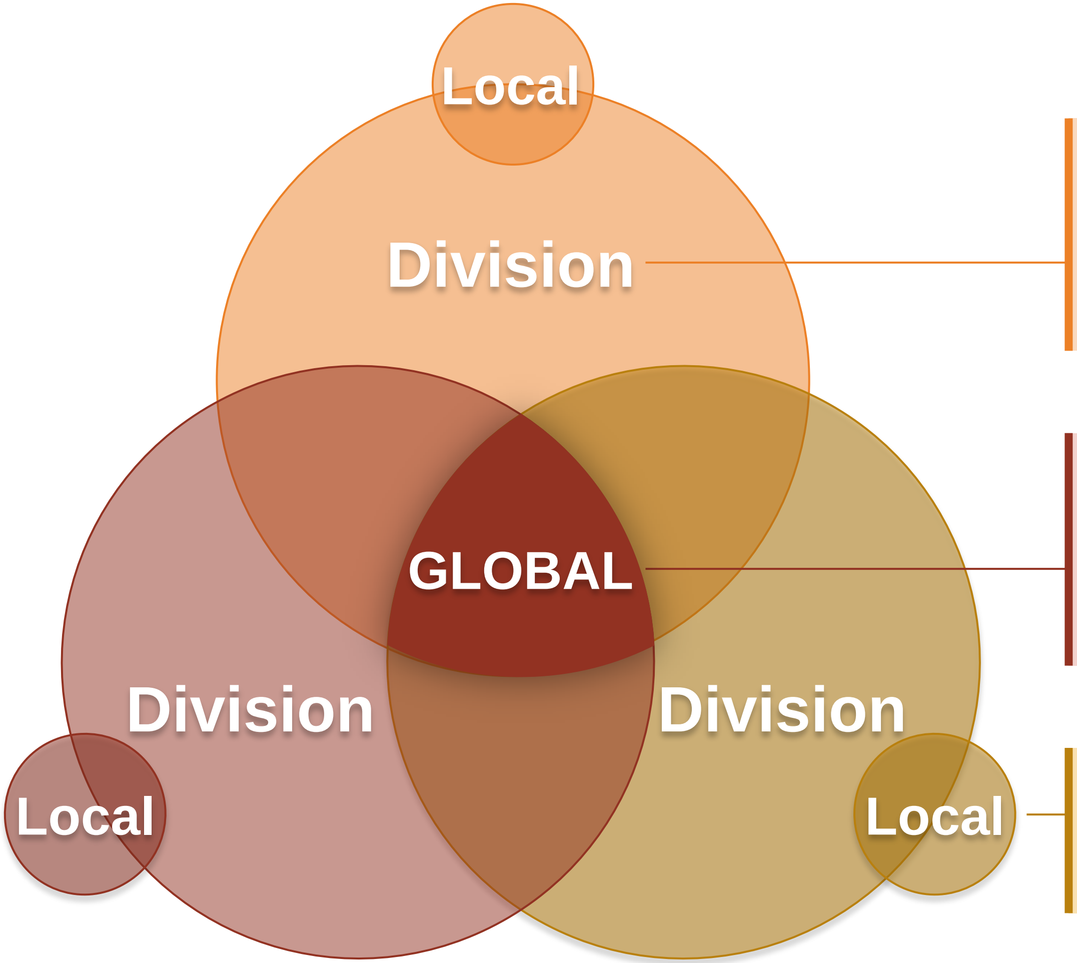
1 Education and Communication

2 Detection and Mitigation of Risks

3 Technology and IT Systems

4 Governance of DI

Establish governance structure

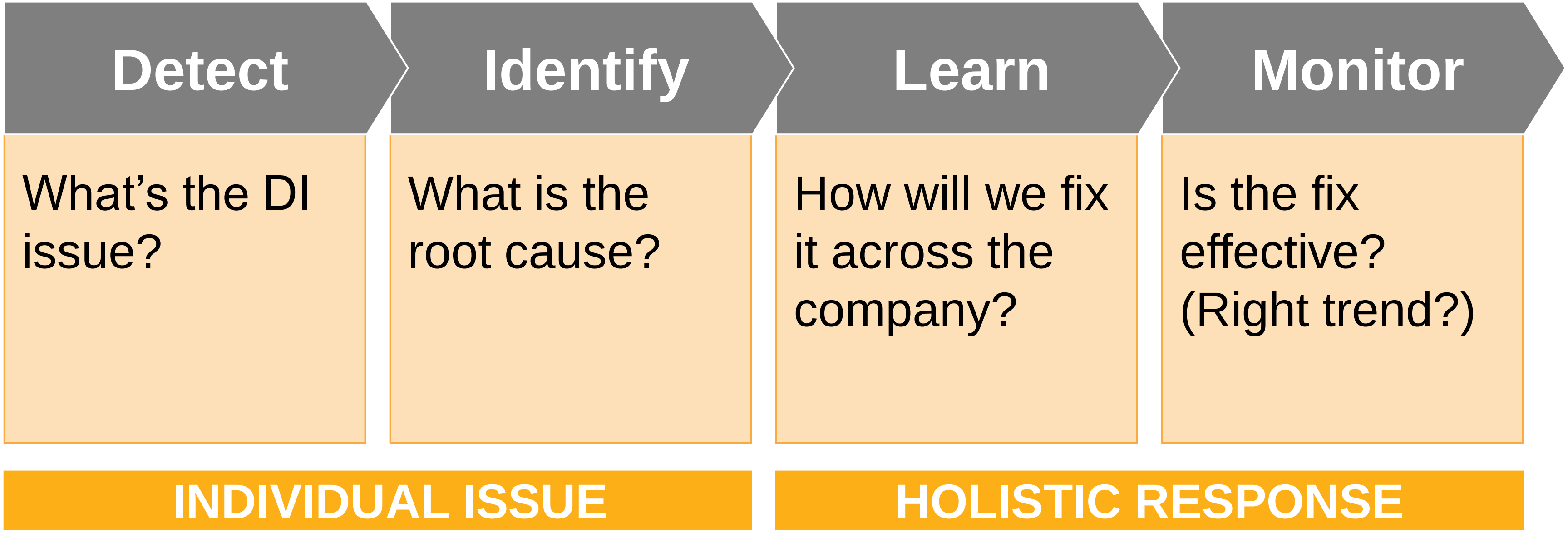


DI Subject Matter Experts provide guidance, recommend improvements

Define DI strategy and standards
Monitor developments internally and externally

Owners of business processes and systems

Establish holistic framework to address DI issues



Detect

What’s the DI issue?

Identify

What is the root cause?

Learn

How will we fix it across the company?

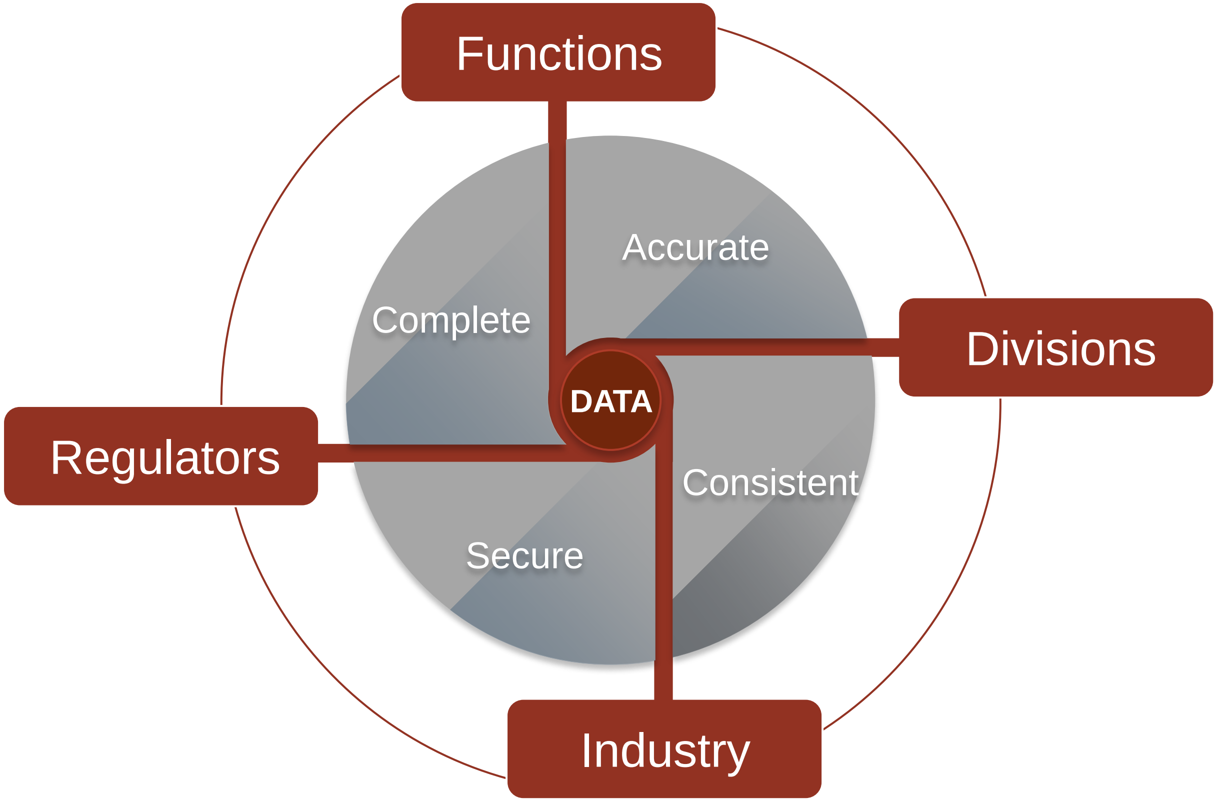
Monitor

Is the fix effective? (Right trend?)

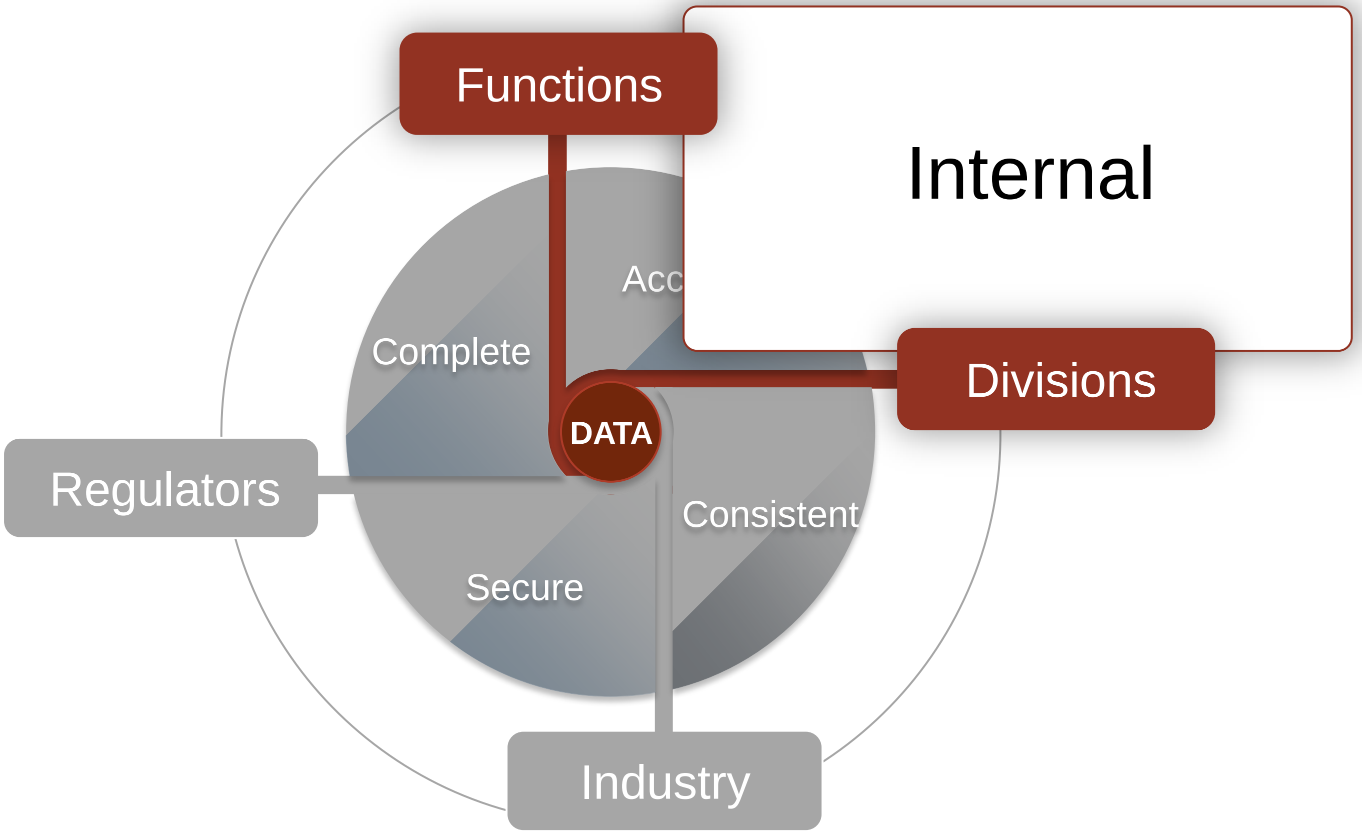
INDIVIDUAL ISSUE

HOLISTIC RESPONSE

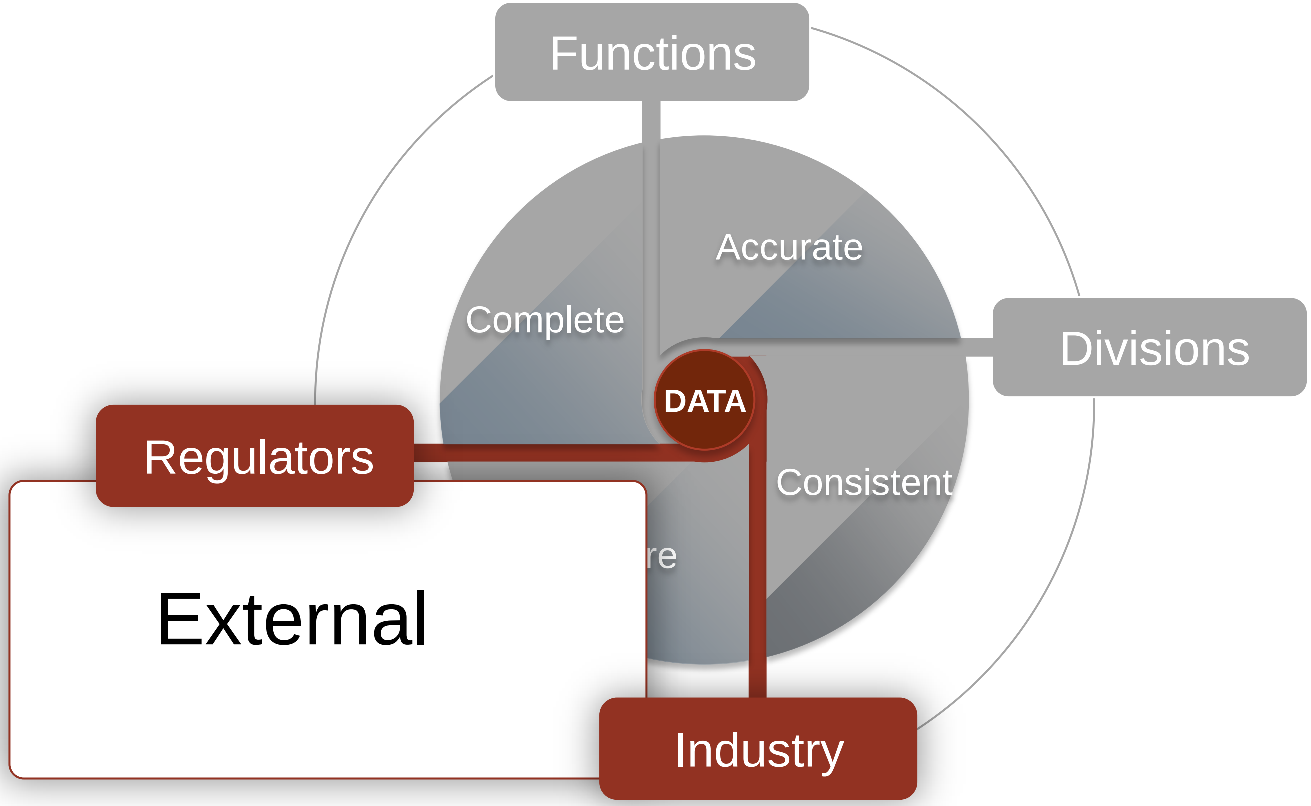
Collaborate to leverage lessons learned



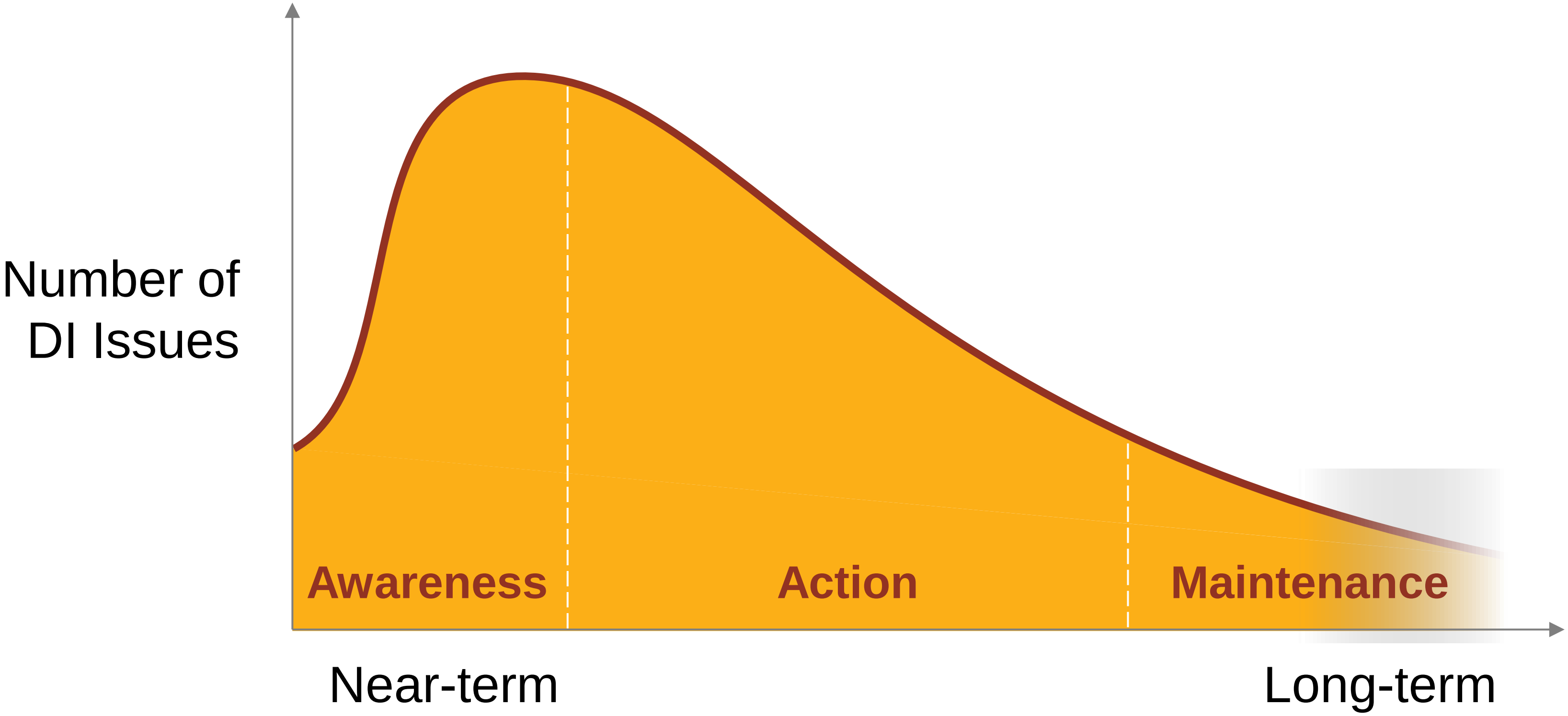
Collaborate to leverage lessons learned



Learn lessons from the industry and regulators



As awareness rises, we'll see more issues at first



Priorities: patient and product quality

Data about safety and efficacy

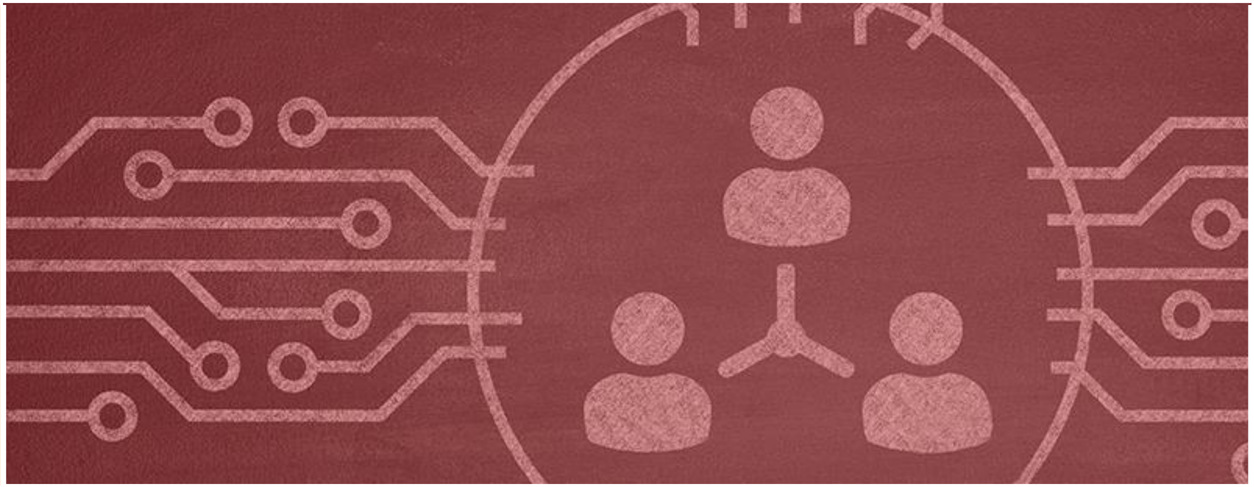
PATIENT

Data that ensures product quality

PRODUCT

Discussion

- How are you prioritizing your DI initiative / activities?
- Where have you chosen to start? Why?



Data Integrity Strategy

Madlene Dole, Head Strategic Planning and Operations - Novartis Group Quality

NOVARTIS

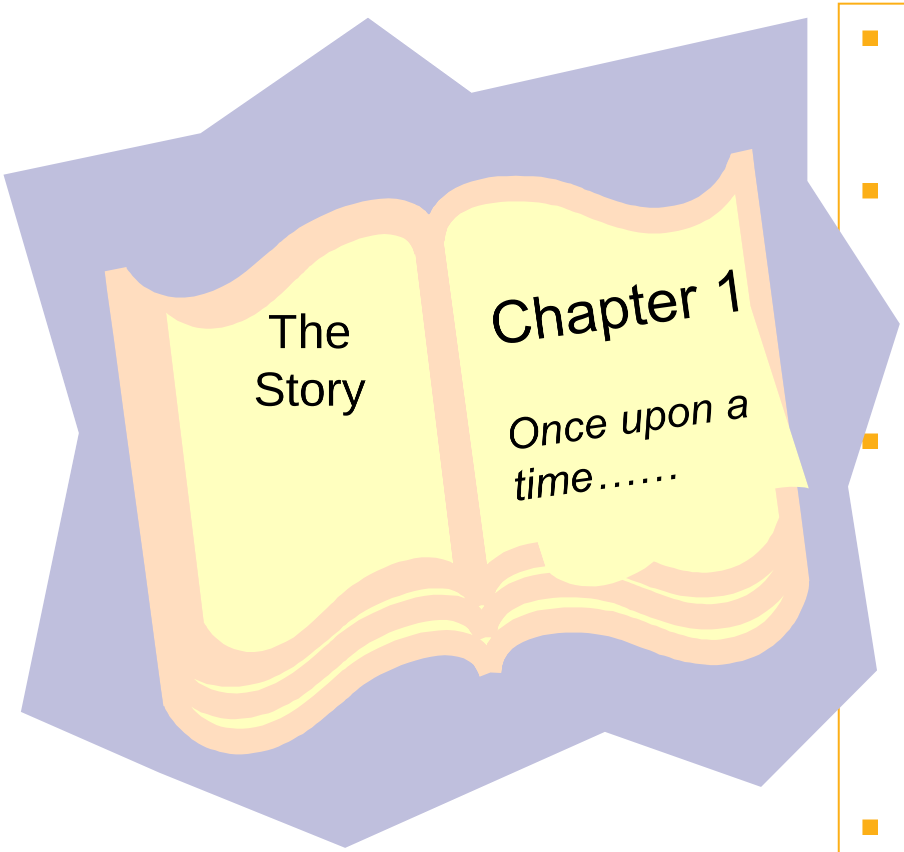
Data Integrity – The Reality

Brendan Walshe. Novartis - Alcon Division.

NOVARTIS

Data Integrity

Background



- Long, Long, time ago in a site far away Discovered:
- Lack of understanding of what is RAW DATA
- Discovered:
  - GDP issues
    - Recording
    - Editing
- Inadequate practices.......

Data Integrity

Background

- **What Quality Systems Impacted?**
  - Data and Record Management
  - Document Management & Change Control
  - Quality Assurance
  - Management Oversight

- **What were the next steps?**
  - **Health Authority** informed
  - **Commitment at a FTF meeting** to **take action on a group level**
    - (data integrity assessments, spot checks, trainings)

Data Integrity

Method

- Workshops/Training
  - How to....
    - Audit Trail Review
    - Group Account Review
- System Inventory
- Assessment Tool
- Audit Guides and Training
- Remediation Plan Template
- Monthly Forum

Data Integrity

The Assessment

- Assessment of Controls Related to Data Management
  - To provide an overview of the data collection systems and the level of electronic and or management controls in place.
  - Used to determine follow-up items, as needed.
  - Applicable to all points of data collection for GMP and GLP systems in the laboratory, development and production (manufacturing) environments.
  - Consisted of a series of questions related to the inventory of electronic systems or processes involving data and the state of controls which are required.
  - The objective of the assessment is to identify controls and data integrity

Data Integrity

The Assessment (Part A)

- Audit trail – active and reviewed
- Part 11 Compliance – how determined
- Raw data (Manf) - is data contained with the batch record and subject to review as part of the release process
- Raw data (Lab) – is data contained with the analytical record and subject to review as part of the release process
- Log Book – audited or verified
- Qualification Status

Data Integrity

The Assessment (Part A)

- User Accounts
  - Passwords controlled and access rights reviewed
  - Accounts personalized
  - Administrator accounts - access restricted according to its business function
  - Are system administrators able to generate, change or even delete data
  - Training

Data Integrity

The Assessment (Part A)

- Non-networked Standalone Systems
  - Data management and control practices
  - Is raw data in the system considered an electronic record and handled/retained accordingly
  - Can reported results be fully traced to source data whether or not it is in paper or electronic form?
  - Is data availability ensured throughout defined retention period even after system retirement
  - Is data backed up and verification ensured

Data Integrity

The Assessment (Part B)

- QA unit relationship to production management
  - QA Unit
    - Describe conditions under which data can be altered, updated, changed, etc., or when equipment controls can be overridden or shut off. How is this communicated to management and documented?
  - In Process Testing
    - Describe how data is collected and what information is maintained with the batch record and what is maintained elsewhere.
  - Availability of Procedures and General Controls
    - Are the relevant SOPs in place for data handling, management, record retention and good documentation practices?

Data Integrity

The Assessment (Part C)

- Manufacturing/Production questions relating to Electronic Signature and Records
  - eCompliance
    - Is ER/ES handled and appropriately managed at the local, operational and equipment level?
  - User Accounts
    - Describe process for maintenance of password controls.
  - Non-networked standalone systems
  - Calibration Management – the process
  - Incident Management – the process
  - Process Validation – the process
  - Change Management – the process

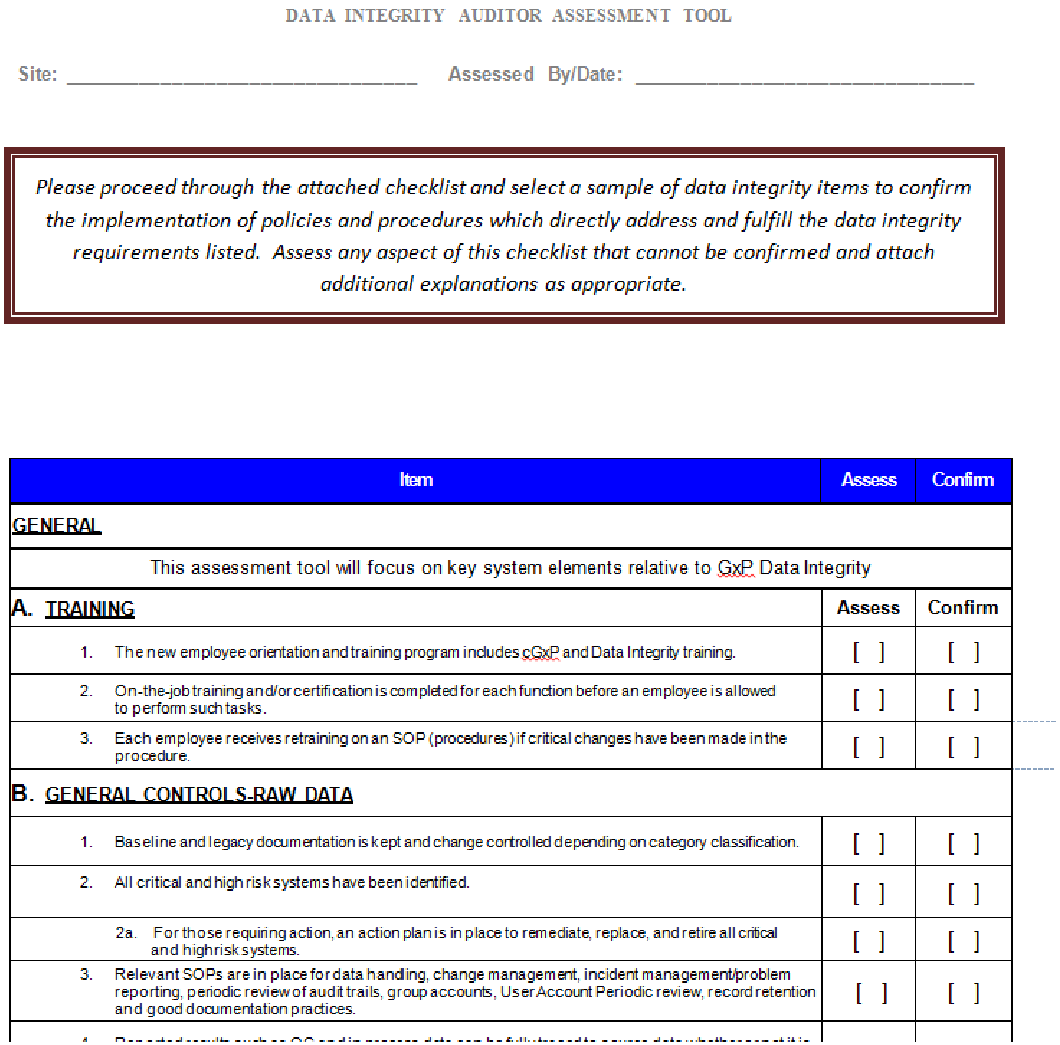
Data Integrity

The Assessment

- Approvers
  - QA Manager
  - eCompliance
  - Business Owners
- Submitted to Division

Data Integrity

Assessment Tool



DATA INTEGRITY AUDITOR ASSESSMENT TOOL

Site: ______________________________ Assessed By/Date: ______________________________

Please proceed through the attached checklist and select a sample of data integrity items to confirm the implementation of policies and procedures which directly address and fulfill the data integrity requirements listed. Assess any aspect of this checklist that cannot be confirmed and attach additional explanations as appropriate.

Item	Assess	Confirm
GENERAL		
This assessment tool will focus on key system elements relative to GxP Data Integrity		
A. TRAINING	**Assess**	**Confirm**
1. The new employee orientation and training program includes cGxP and Data Integrity training.	[ ]	[ ]
2. On-the-job training and/or certification is completed for each function before an employee is allowed to perform such tasks.	[ ]	[ ]
3. Each employee receives retraining on an SOP (procedures) if critical changes have been made in the procedure.	[ ]	[ ]
B. GENERAL CONTROLS-RAW DATA		
1. Baseline and legacy documentation is kept and change controlled depending on category classification.	[ ]	[ ]
2. All critical and high risk systems have been identified.	[ ]	[ ]
2a. For those requiring action, an action plan is in place to remediate, replace, and retire all critical and high risk systems.	[ ]	[ ]
3. Relevant SOPs are in place for data handling, change management, incident management/problem reporting, periodic review of audit trails, group accounts, User Account Periodic review, record retention and good documentation practices.	[ ]	[ ]
4. Reported results such as QC and in-process data can be fully traced to source data whether or not it is		

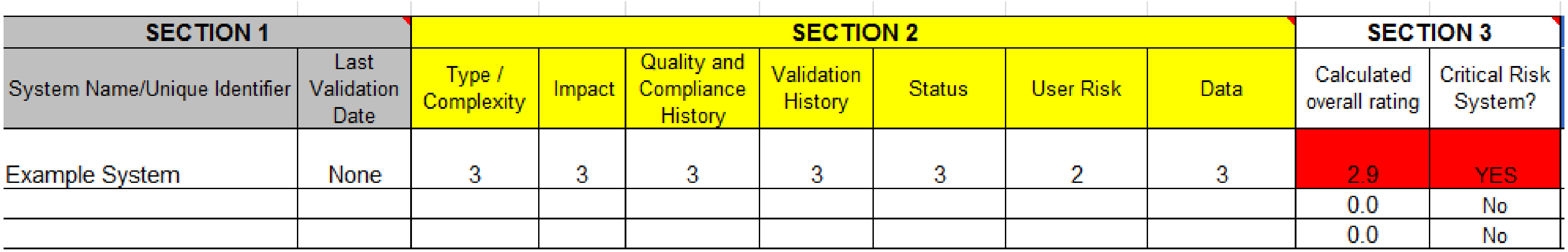
Data Integrity

DI Risk Prioritization and Remediation Plan

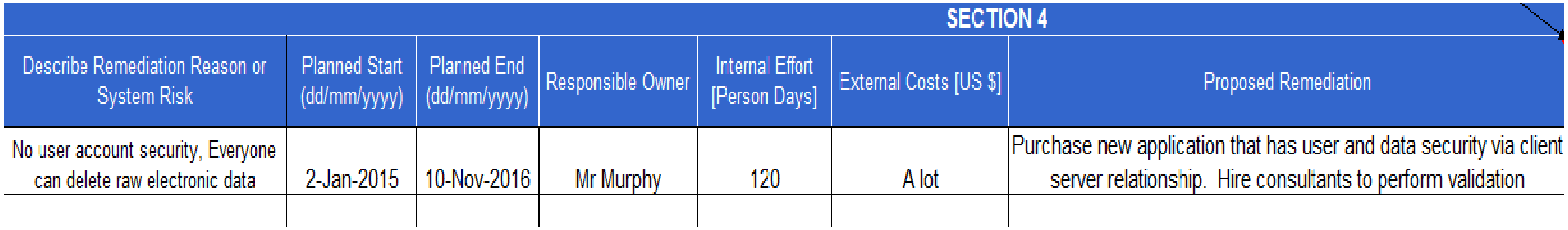
- Section 1: Inventory List
- SECTION 2: Assess risks as low (1), medium (2) and high (3) for each of 7 categories as per General Rules
- System Type/Impact of Failure/Compliance History
- SECTION 3: Overall Rating Calculated and Critical Systems Identified
- Remediation section with expected dates, responsible project owner, internal effort in person days, estimated costs, etc.

Data Integrity – Example System

DI Risk Prioritization and Remediation Plan



SECTION 1		SECTION 2							SECTION 3	
System Name/Unique Identifier	Last Validation Date	Type / Complexity	Impact	Quality and Compliance History	Validation History	Status	User Risk	Data	Calculated overall rating	Critical Risk System?
Example System	None	3	3	3	3	3	2	3	2.9	YES
									0.0	No
									0.0	No



SECTION 4						
Describe Remediation Reason or System Risk	Planned Start (dd/mm/yyyy)	Planned End (dd/mm/yyyy)	Responsible Owner	Internal Effort [Person Days]	External Costs [US $]	Proposed Remediation
No user account security, Everyone can delete raw electronic data	2-Jan-2015	10-Nov-2016	Mr Murphy	120	A lot	Purchase new application that has user and data security via client server relationship. Hire consultants to perform validation

Data Integrity

DI Plan - Actions

- Process to review User access and document User control
- Update System Configuration
- System Replacement
- Perform Periodic Review
- System Upgrade
- Documentation
- Implement unique login

Data Integrity
Results

- Assessment Completed and Plan Approved (V1)
- Division oversight, Forum, Monthly Reporting.
- Audit – interpretation
- “Is raw data in the system considered an electronic record and handled/retained accordingly? “
- CAPAs - Re-execute the assessment
- Build into existing Process(s)
- Education...Education..

Data Integrity

What we have learned

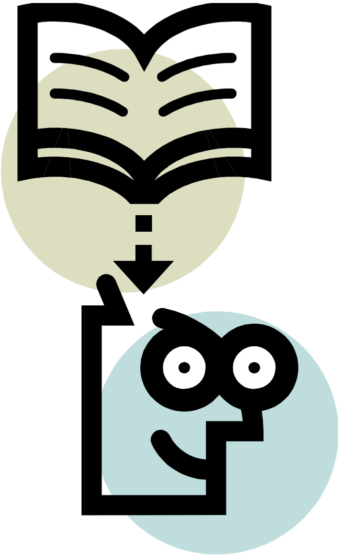
- Controls must be in place to ensure the integrity of data
- A well prepared GxP document provides objective evidence of an “action” and the result of an “action”
- Why it is critical to ensure data is accurate and controlled
- Data must be safe from manipulation or loss, intentional or unintentional
- It is critical to educate personnel on data integrity and its overall impact on product identity, strength, purity and safety.

What have we learned?

Data Integrity

What we have learned

Data Handling is key to Data Integrity



We must consider:

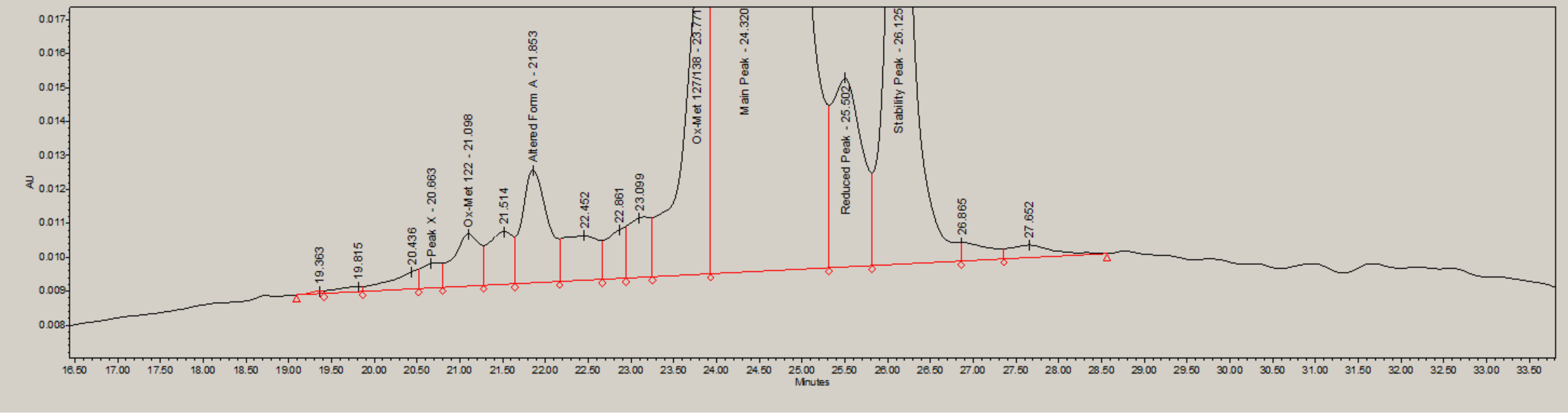
- How data is **collected** and **reported**
- How data is **reviewed**
- How the integrity of data is **protected**
- How **calculation errors** are handled
- How **alarms** are managed
- Who has the authority to **invalidate data**
  - » What happens to this data? (i.e., discarded, archived with sample analysis package, etc.)
- How electronic data is **protected** from editing, changing, deletion?
  - » How are passwords assigned and protected?

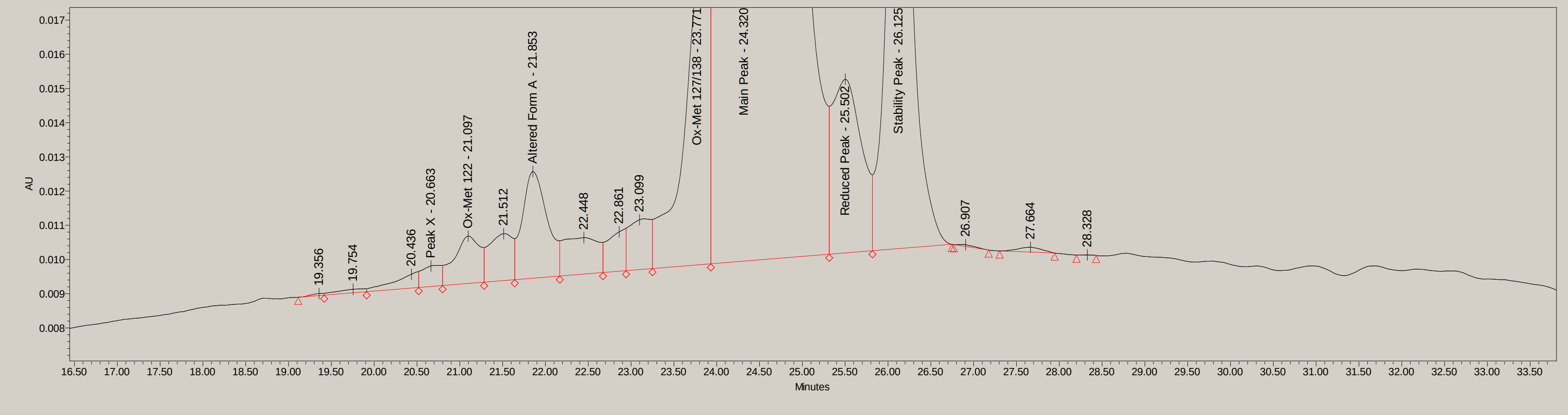
Thank You

Data Integrity means the data are complete, consistent, accurate, and secure. It means the data are reliable.

Backup Slides

Backup – Subtle Integration Example


AU
Peak X - 20.663
Ox-Met 122 - 21.098
Altered Form A - 21.853
Ox-Met 127/138 - 23.771
Main Peak - 24.320
Reduced Peak - 25.502
Stability Peak - 26.125
Minutes


AU
Peak X - 20.663
Ox-Met 122 - 21.097
Altered Form A - 21.853
Ox-Met 127/138 - 23.771
Main Peak - 24.320
Reduced Peak - 25.502
Stability Peak - 26.125
Minutes