Establishing a Data Integrity Assurance program

Chinmoy Roy
chinmoyr@gmail.com
(510) 676 1995

CCP1 (Vacaville) Groundbreaking

Agenda

- Fundamental concepts
- The “least burdensome approach”
- Data Integrity Controls Triad
- Data Integrity’s 5-p model
- Data Integrity risk assessment

Let us explore some basic concepts such as data, data integrity before we proceed to establish a Data Integrity program

What is Data Integrity

Data Integrity is the assurance that data is accurate, complete and maintained within the original context so as to make the data trustworthy

DI definitions by agency guidance

USFDA	Completeness, consistency and accuracy and satisfy ALCOA
MHRA	The extent to which all data are complete, consistent and accurate throughout the data lifecycle.
WHO	Degree to which complete, consistent and accurate. Conform to ALCOA throughout lifecycle. Adherence to sound scientific principles and GDP
PICS	Extent to which data is complete, consistent and accurate throughout the data lifecycle
TGA	Data Integrity is defined as "the extent to which all data are complete, consistent and accurate, throughout the data lifecycle"

Guiding principles of Data Integrity

Ensure the continuous care, custody and control of systems and data

Why DI issues occur

- **Improper Practice**

  A scientifically unsound or technically unjustified omission, manipulation, or alteration of procedures

- **Fraud**

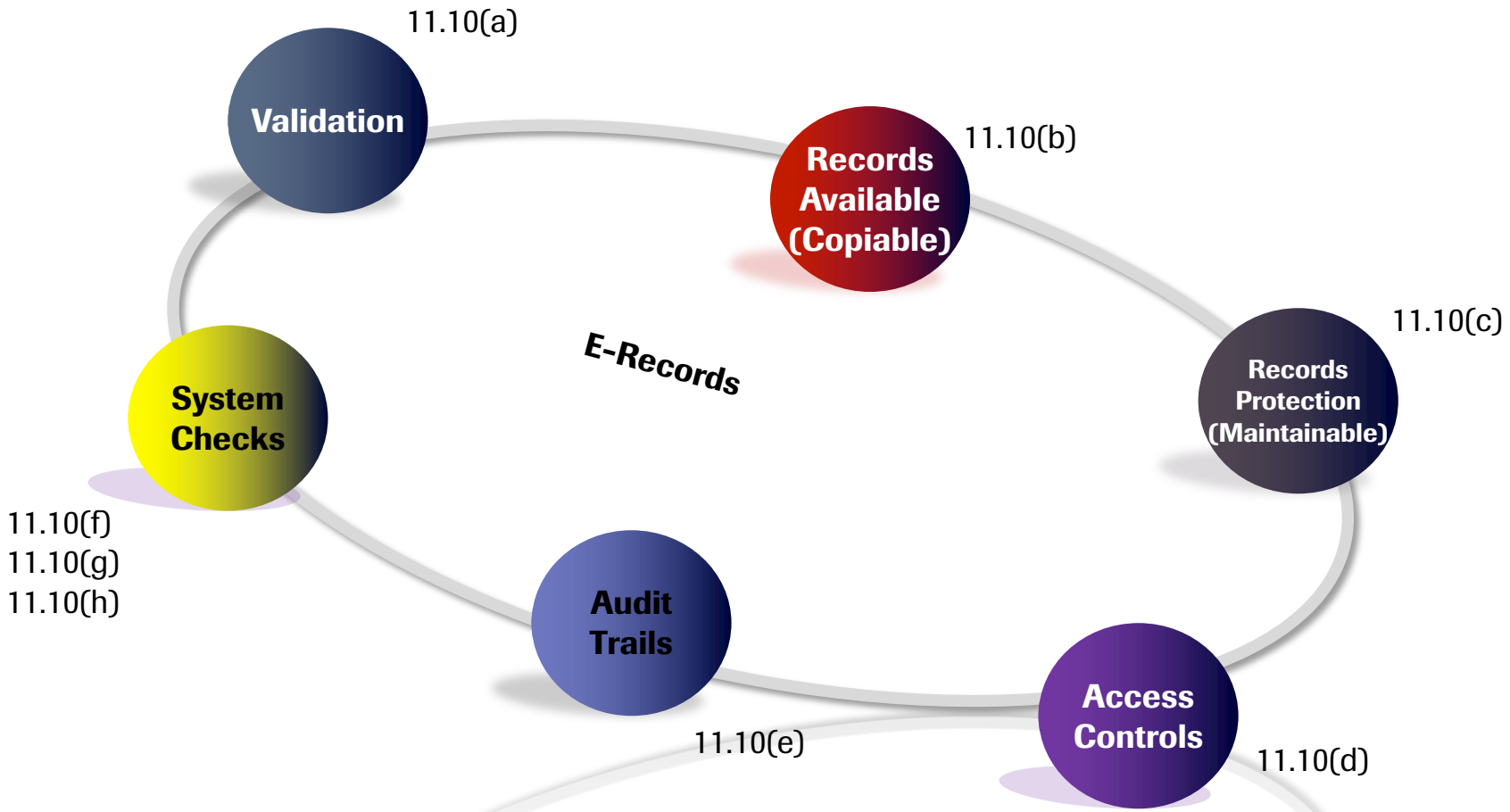
  The deliberate falsification of data/results, where failed method requirements are made to appear acceptable during reporting.

- **Errors, slips lapses**

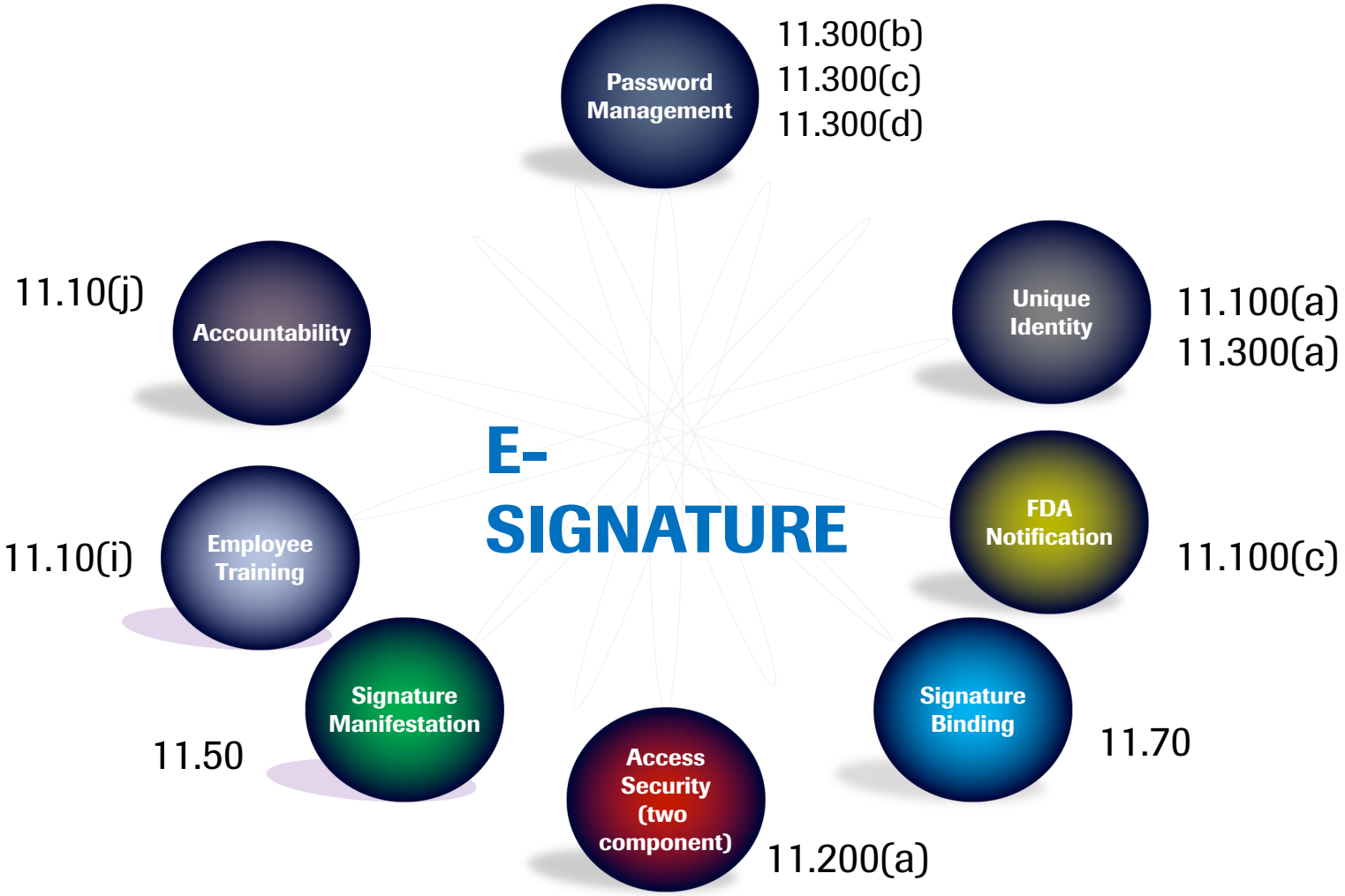
Integrity characteristics of data

- **ALCOA**: Stan Woolen in early 1990's came up with this acronym to fight off public speaking jitters
- Over time it evolved into ALOCA+
- The + elements are Complete, Consistent, Enduring and Available

Part 11: Electronic Records



Part 11: Electronic Signatures



So what do mean by “the least burdensome approach”

How to apply to a DI program

- Look at “Part 11 Scope and Application” guidance
- Understand the “tag along audit” guidance that FDA provided their field inspectors
- Read up CPG 7346.832 (PAI)
- Look up USFDA’s Data Integrity guidance
- Look at the history of WL and 483s and verify audit trends conform to those mentioned above

Excerpt: Part 11 "Scope and Application"

- **Narrowly interpret scope where fewer records will considered subject to Part 11**
- **We intend to exercise enforcement discretion with regards to Part 11 requirements for the following:**
  - validation
  - access control
  - audit trails
  - change control

Understand "tag along audit" objectives

- **Data integrity associated items that regulators are trained on to look for during regular audits:**
  - Raw data availability
  - Vendor and supplier audit reports
  - Calibrate and validate equipment and software
  - Access control
  - Input/output accuracy
  - Audit trails
  - Change control

Understand CPG 7346.832 (PAI)

- **Objective 3: Data Integrity audit**
  - Audit the raw data for completeness, accuracy so that agency can rely on the submitted data
  - Specifically data on finished product quality, dissolution, content uniformity and stability
  - Instruments calibrated, software and equipment validated

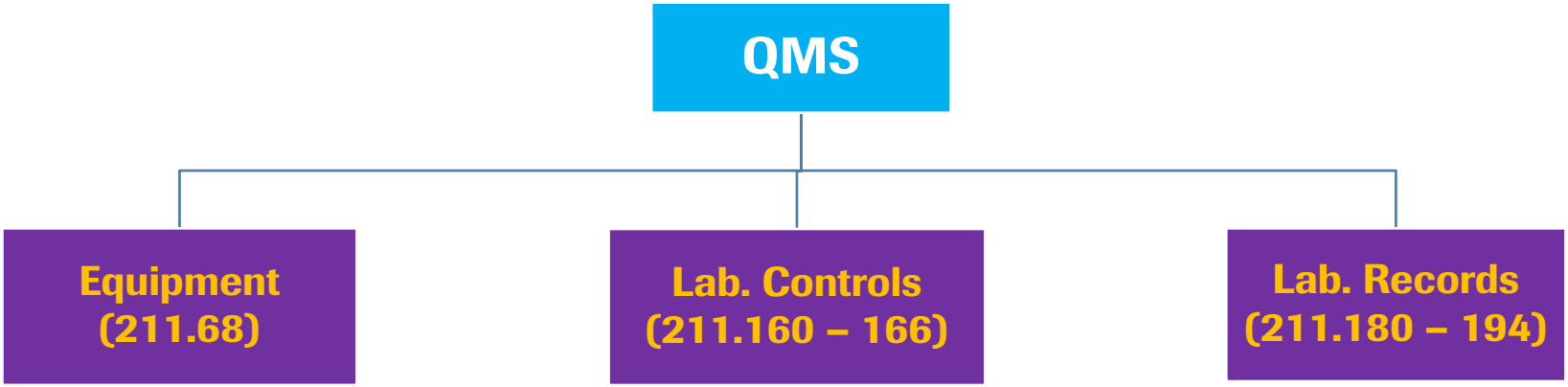
Review FDA's DI guidance

regarding safety, identity, strength, quality, and purity." Requirements with respect to data integrity in parts 211 and 212 include, among other things:

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

Electronic signature and record-keeping requirements are laid out in 21 CFR part 11 and apply to certain records subject to records requirements set forth in Agency regulations, including parts 210, 211, and 212. For more information, see guidance for industry *Part 11, Electronic Records; Electronic Signatures — Scope and Application*.[3] The guidance outlines FDA's current thinking regarding the narrow scope and application of part 11 pending FDA's reexamination of part 11 as it applies to all FDA-regulated products.

DI WL: 3 categories

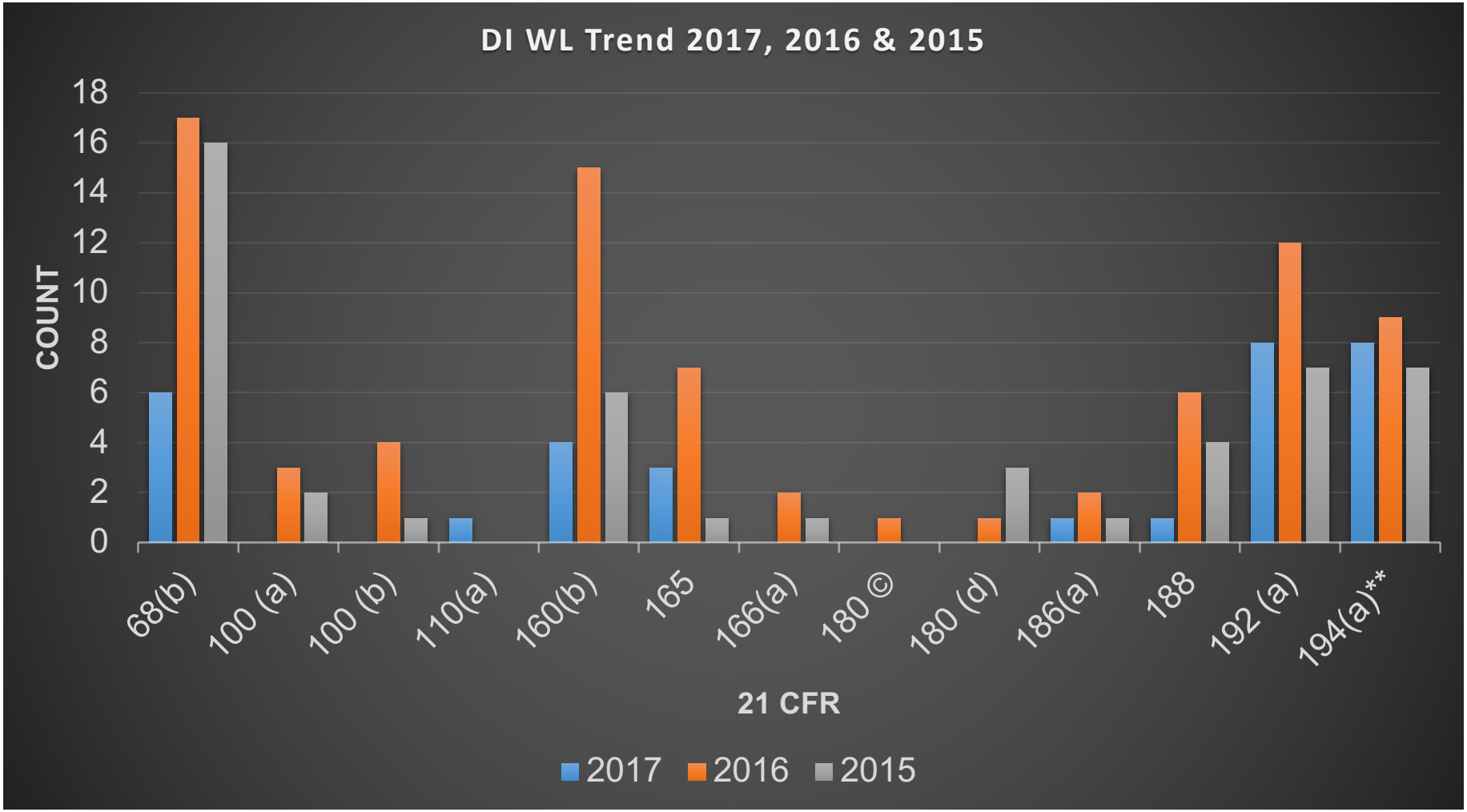


- Shared identities
- Inappropriate access privileges
- No backup & restore procedure
- Data deleted or lost
- Calculations not validated

- No Man. Integ. guidance
- Unofficial testing
- No reprocess. guidance
- No stability testing
- No procedures eg sample
- Not scientifically sound

- Incomplete data
- No batch record reviews
- No OOS done
- Data falsification
- Methods not validated
- No second person check

DI warning letters trends



Top 4 DI citations in 2016 & 2017

2017

- OOS
- Complete data
- Access control
- Laboratory control

2016

- Access control
- Laboratory controls
- OOS
- Complete data

DI guidance & their directives

Description summary		DI Directives/SOP
Backup data exact, complete, secure, calibration, validation	§ 211.68	▪ Validation ▪ Calibration ▪ GDP ▪ Access control ▪ Audit Trail review
Data stored to prevent deterioration or loss	§ 212.110(b)	▪ Data backup and recovery ▪ Business Continuity ▪ Data migration and archiving
Contemporaneous	§ 211.100	▪ Date and Time ▪ GDP
Laboratory controls, “scientifically sound”	§ 211.160	▪ Laboratory Controls ▪ Validation ▪ Calibration ▪ GDP

DI guidance & their directives

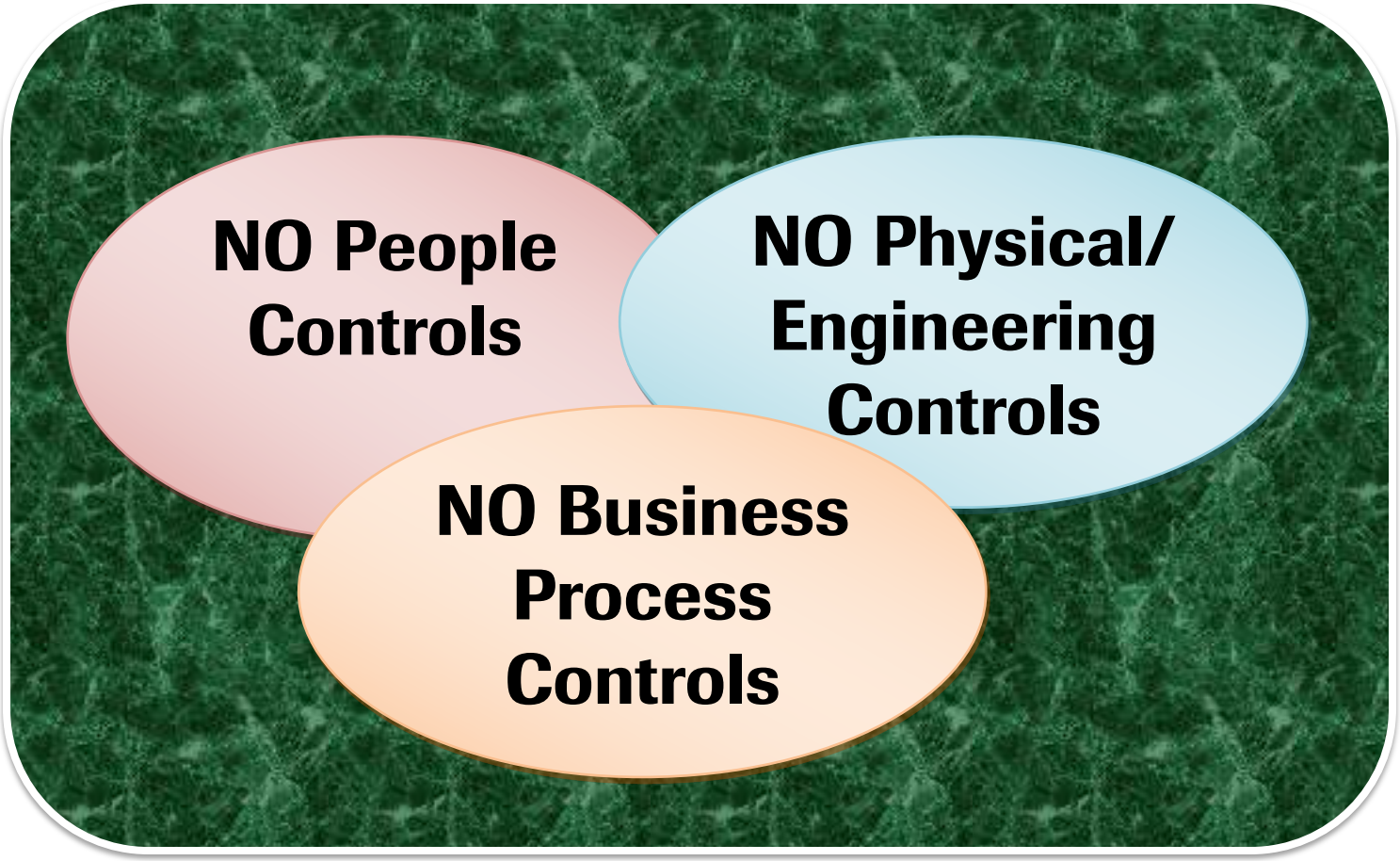
Description summary		DI Directives/SOP
Raw data available	§ 211.180	▪ Raw Data & Metadata retention
Contemporaneous	§ 211.188	▪ Date and Time ▪ GDP
Investigate OOS	§ 211.192	▪ OOS
Complete test results	§ 211.194	▪ GDP ▪ Lab controls ▪ Manual Data entry

Data Integrity Controls Triad

Data Integrity Controls Triad

- **These controls mitigate occurrence of DI issues**
  - Management controls
  - Procedural controls
  - Technical controls
- **Management controls influence the Attitude**
- **Procedural controls impact the Incentive**
- **Technical controls reduces the Opportunity**

Why DI problems occur



Data Integrity's 5-p model

What is 5-p model

A strategic model that requires alignment of all 5 parameters (5-p) to improve operations and achieving business goals

What is DI's 5-p model

The 5-p are:

- **P**urpose (policy)
- **P**rinciples (ethics, code of conduct)
- **P**rocesses (directives / SOPs)
- **P**eople (governance, management)
- **P**erformance (maturity model, metrics)

What is DI's 5-p model

The 5-p are:

- **Purpose (policy)**
- Principles (ethics, code of conduct)
- Processes (directives / SOPs)
- People (roles & responsibilities)
- Performance (metrics)

DI Policy

1. Purpose

This Data Integrity Quality Policy states Biotech's Corporate Quality requirements for the custody and control of Biotech's data and information assets that are required to meet regulatory requirements. It is based on industry best practices to meet needs in a cGMP environment. The major reasons for establishing a single quality policy for data integrity are:

Ethics Provide rules of conduct to assure data integrity

Control Provide a standardized framework for management and control of data

Law Establish accountability, inspection readiness and consistent compliance with regulatory authorities.

This policy is also intended to do the following:

- Provide Biotech personnel at a high level, clear and consistent guidance to ensure data integrity and minimize Biotech's exposure to risks in a regulated environment.
- Stress the high degree of importance to data integrity by Biotech's management
- Emphasize Biotech management's involvement in following up on observations and concerns of data integrity breaches and issues

2. Scope

This policy applies to all data collected from the following regulated or cGxP operations:

- Manufacturing, controlling, testing, packaging, holding or distributing drugs for human use
- Create, modify, maintain, archive, retrieve or transmit data that may be included in a submission to a regulatory authority or used to make regulatory decisions

DI Policy..... contd

3. Policy Statement

1. Biotech considers all data as corporate assets and relies on its' accuracy, completeness and trustworthiness to make decisions to achieve business goals.
2. Data that impacts GxP processes need to be identified along with the designated data owners who ensure that the data is validated and is maintained in a validated state at all times.
3. The data owner is ultimately responsible for the validation, continuous security and authenticity of the data throughout the data's lifecycle.
4. Any additional application-specific data requirements such as data quality, security etc. should be addressed within local documentation such as SOPs and Instructions.
5. Existing non-validated systems in use that come into the scope of this policy because of changing regulatory requirements or a change in intended use must be evaluated for compliance and validated, if required.
6. Management involvement with ensuring the integrity of all GxP impact data is mandatory.
7. Biotech recognizes that the ethics of its personnel is key to ensuring data integrity within the enterprise. Hence it is mandatory for all its employees to sign the Ethics Agreement as a condition of employment.
8. Every employee shall undergo Ethics training where Biotech's ethics agreement and policy shall be explained.
9. Every employee shall be required to undergo a mandatory refresher training in Ethics at least once every year

DI Policy..... contd

10. Biotech incentivizes every employee to directly report any and all instances of suspected violations of Data Integrity to the CEO directly with no fear of retribution or threat of termination of employment at Biotech.
11. Any wilful breach of data integrity with intention to defraud or misrepresent data by any employee shall result in the summary termination of employment at Biotech.

What is DI's 5-p model

The 5-p are:

- Purpose (policy)
- Principles (ethics, code of conduct)
- **Processes (directives / SOPs)**
- People (roles & responsibilities)
- Performance (metrics)

Processes

Attributable	Access Control, Data & Time, Audit Trail design
Legible	Good Documentation Practices (GDP)
Contemporaneous	Date and Time, GDP
Original	Raw Data & Metadata retention
Accurate	Calibration, Laboratory Controls, Change Controls, Deviation & Incident management,, Validation, OOS
Complete	Laboratory Controls, GDP, Manual data entry
Consistent	Validation, Audit Trail review, SDLC, Electronic records management, Manual Integration guidance
Enduring	Data Backup & Recovery, Audit Trail design
Available	Business Continuity, Data Backup & Recovery, Data Migration and Archiving, Building Monitoring System design

What is DI's 5-p model

The 5-p are:

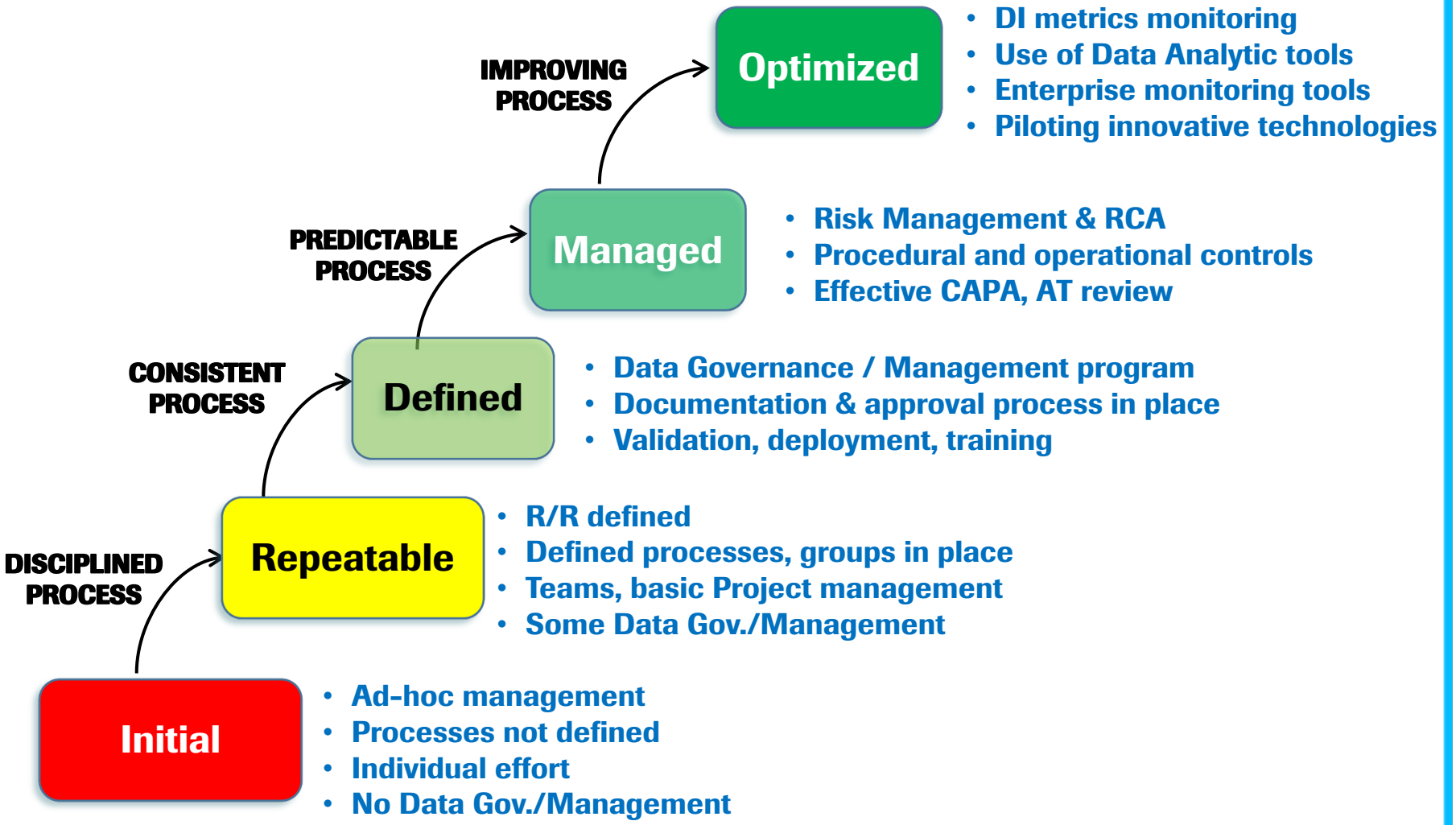
- Purpose (policy)
- Principles (ethics, code of conduct)
- Processes (directives / SOPs)
- People (roles & responsibilities)
- **Performance (metrics)**

Data Integrity Maturity Model

- **Based on CMU/SEI's CMM for Software**
- **Consists of 5 levels of increasing maturity**
  - Initial / Ignorance*
  - Repeatable / Denial*
  - Defined / Understanding*
  - Managed / Policing*
  - Optimized / Maturity*
- **Understand process activities required to reach level demonstrates continuous improvement, a ICH Q10 hallmark**

*: courtesy Mr. David Churchward, MHRA

Data Integrity Maturity Model

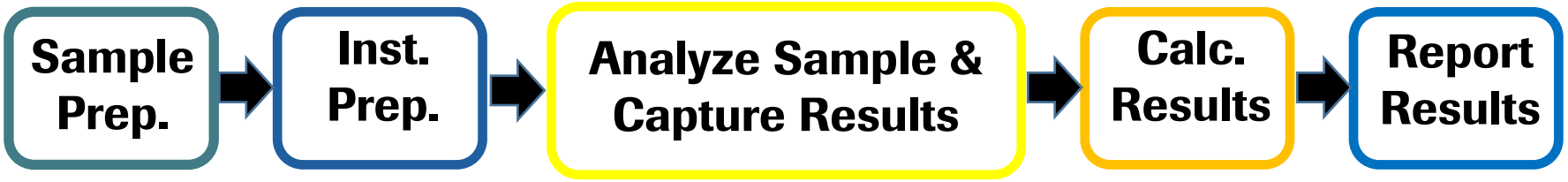


Data Integrity Risk Assessment; not ICH Q9

Data Integrity risk assessment

- **Useful approach is to “map the workflow”**
- **For each step of workflow, identify the following:**
  - What actions are performed
  - How those actions are performed
  - How they are recorded
  - What decisions if any are made at that step
  - The extent to which step is manual or automated
  - Fraud potential and their prevention

Identify the process steps



Specify actions at each step

- **Collect sample**
- **Document**
  - ✓ Batch ID
  - ✓ Weight
  - ✓ Dilution
  - ✓ Inst. ID

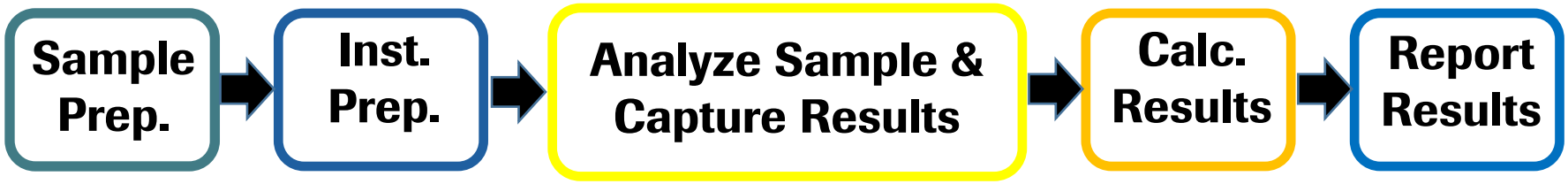
- **Follow defined procedure**
- **Set oper. parameters**
- **Record & report results**

- **Injection sequence**
- **What data to capture**
- **Link to methods & formulas used**
- **Save data**
- **Save reanalysis data if any**

- **Save results**
- **Link to formulas used**
- **Manual integration**

- **Second person review of results**
- **Retain raw data**

Associate DI related activities



- Record data per SOP
- Anal. name, date time
- Verify raw data
- Prep sample as per SOP
- Save prep data
- Ensure data unerasable

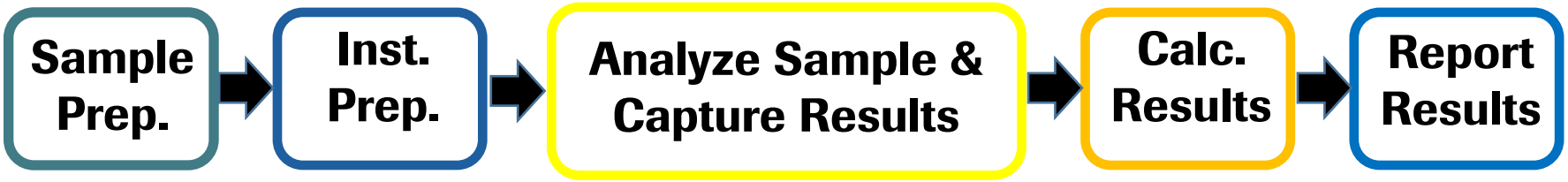
- Prep as per SOP
- Record & save prep data
- Ensure data unerasable

- Ref. Std. SOP
- Ensure Methods validated
- Raw data saved and unerasable
- Save data
- Save reanalysis data if any

- SOPs: man. Integ., aberrant data in place
- Alg & routines validated
- Complete data
- All data saved and cannot be erased

- Second person review of results
- Review SOP in place
- Retain raw data
- Reports stored and easily available

Identify the data operations



- Acquire
- Enter
- Store

- Enter
- Edit
- Copy

- Acquire
- Store
- Process
- Copy

- Process
- Store
- Edit
- Delete
- Copy

- Copy
- Enter
- Move
- Store
- Edit

Data operations risks & mitigation

Data Action	Risk	Mitigation
Data Acq.	Inaccurate measurement	Trained staff, calibration SOP
Data Entry	Human, transposition error or fraud	Staff training, authenticate user
Data storage	Media failure, modification	Suitable SOPs for secure, redundant and encrypted data storage
Data Editing	Human/transposition error, fraud	Change control, enabled audit trails, access control
Data proc.	Erroneous processing software	Validate software
Data copying	Not fully copied (such as metadata)	Validate copy function, verify move
Data delete	Accidental, fraudster, not physically deleted	Trained staff, change control, validate delete
Data move	Improper copied data, moved to wrong place	Trained staff, validate copy

Typical DI RA results

Step Name	Data Operation	Risk (Y/N)	Mitigation
Sample Prep	Acquire	Y	Train staff on SOP
	Entry	Y	Provide secound pair of eyes
	Storage	N	N/A
Instrument Prep	Entry	Y	In SOP, specify to ensure that audit trails are turned on
	Edit	Y	Ensure analyst cannot edit data and only authorized personnel can
	Copy	N	N/A
Analyze sample & Capture results	Acquire	Y	Validate inst. config, calibration
	Storage	N	N/A
	Process	Y	Validate method, formulas
	Copy	N	N/A

End of slide deck