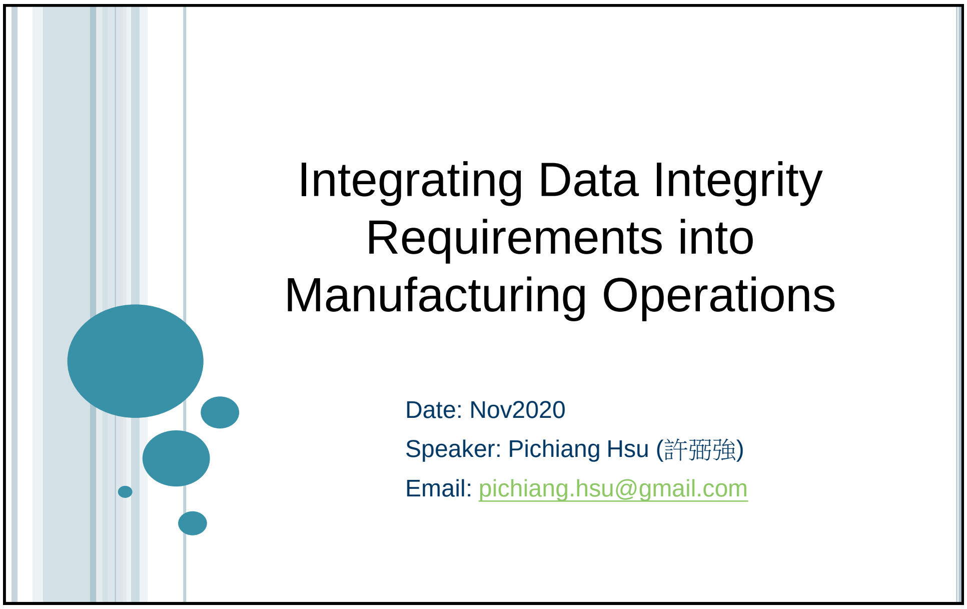
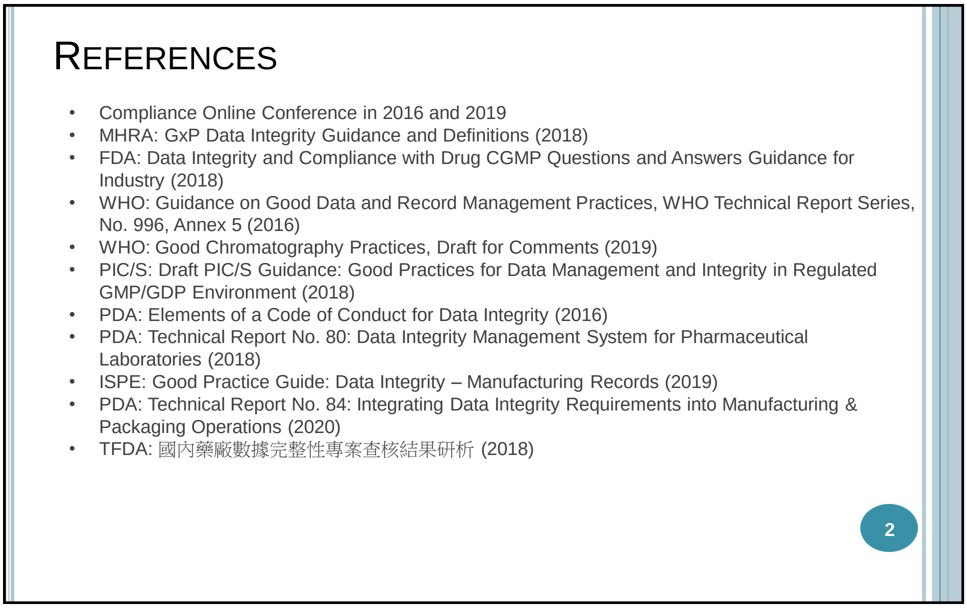


Integrating Data Integrity Requirements into Manufacturing Operations

Date: Nov2020

Speaker: Pichiang Hsu (許弼強)

Email: pichiang.hsu@gmail.com



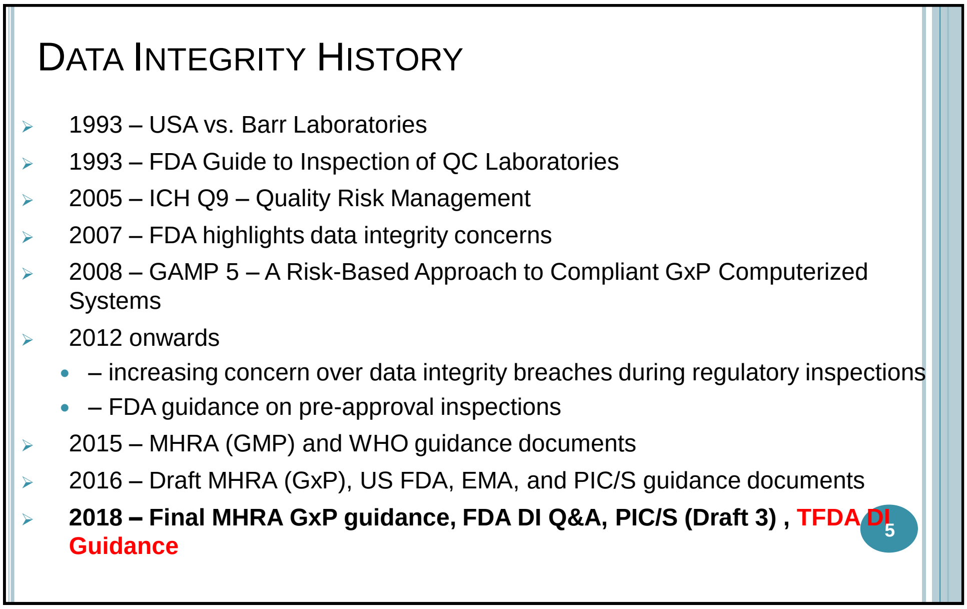
REFERENCES

- Compliance Online Conference in 2016 and 2019
- MHRA: GxP Data Integrity Guidance and Definitions (2018)
- FDA: Data Integrity and Compliance with Drug CGMP Questions and Answers Guidance for Industry (2018)
- WHO: Guidance on Good Data and Record Management Practices, WHO Technical Report Series, No. 996, Annex 5 (2016)
- WHO: Good Chromatography Practices, Draft for Comments (2019)
- PIC/S: Draft PIC/S Guidance: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environment (2018)
- PDA: Elements of a Code of Conduct for Data Integrity (2016)
- PDA: Technical Report No. 80: Data Integrity Management System for Pharmaceutical Laboratories (2018)
- ISPE: Good Practice Guide: Data Integrity – Manufacturing Records (2019)
- PDA: Technical Report No. 84: Integrating Data Integrity Requirements into Manufacturing & Packaging Operations (2020)
- TFDA: 國內藥廠數據完整性專案查核結果研析 (2018)

Agenda

- Data integrity historical background
- Data integrity definitions and regulatory requirements
- Data integrity risk assessment
- Data integrity controls
- Computerized systems

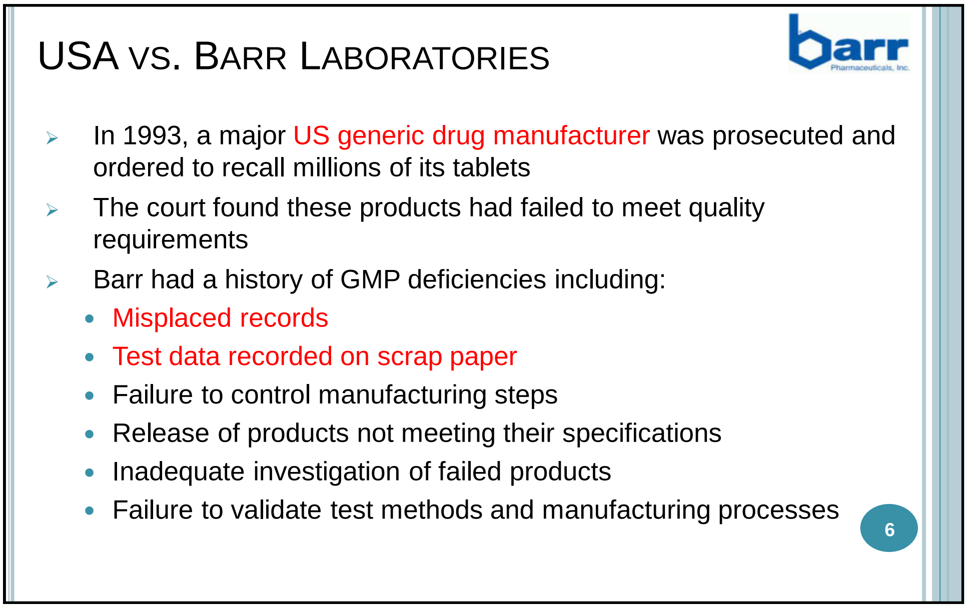
Data Integrity Historical Background



Data Integrity History

- 1993 – USA vs. Barr Laboratories
- 1993 – FDA Guide to Inspection of QC Laboratories
- 2005 – ICH Q9 – Quality Risk Management
- 2007 – FDA highlights data integrity concerns
- 2008 – GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems
- 2012 onwards
  - – increasing concern over data integrity breaches during regulatory inspections
  - – FDA guidance on pre-approval inspections
- 2015 – MHRA (GMP) and WHO guidance documents
- 2016 – Draft MHRA (GxP), US FDA, EMA, and PIC/S guidance documents
- **2018 – Final MHRA GxP guidance, FDA DI Q&A, PIC/S (Draft 3) , TFDA DI Guidance**

5

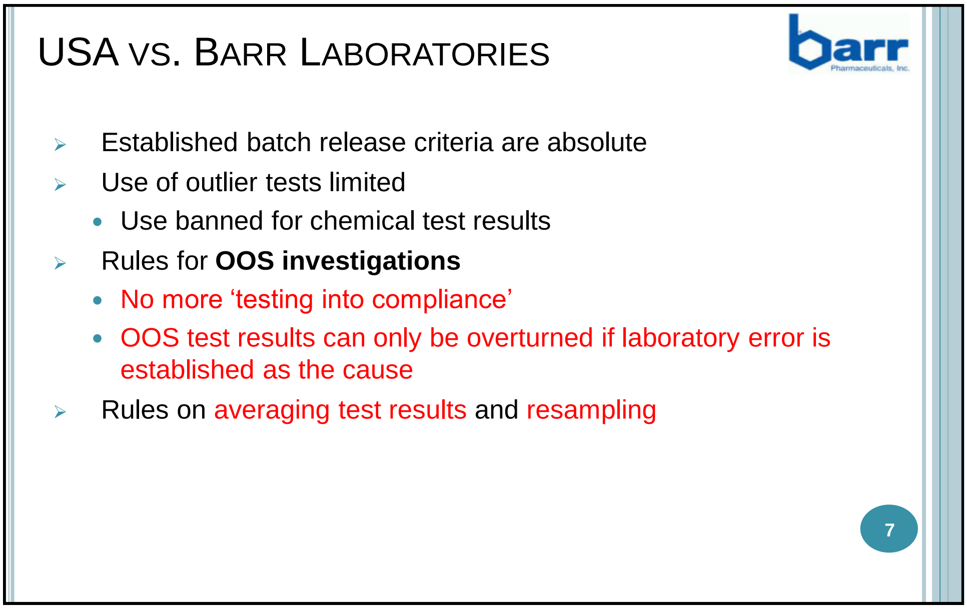


USA vs. Barr Laboratories

barr
Pharmaceuticals, Inc.

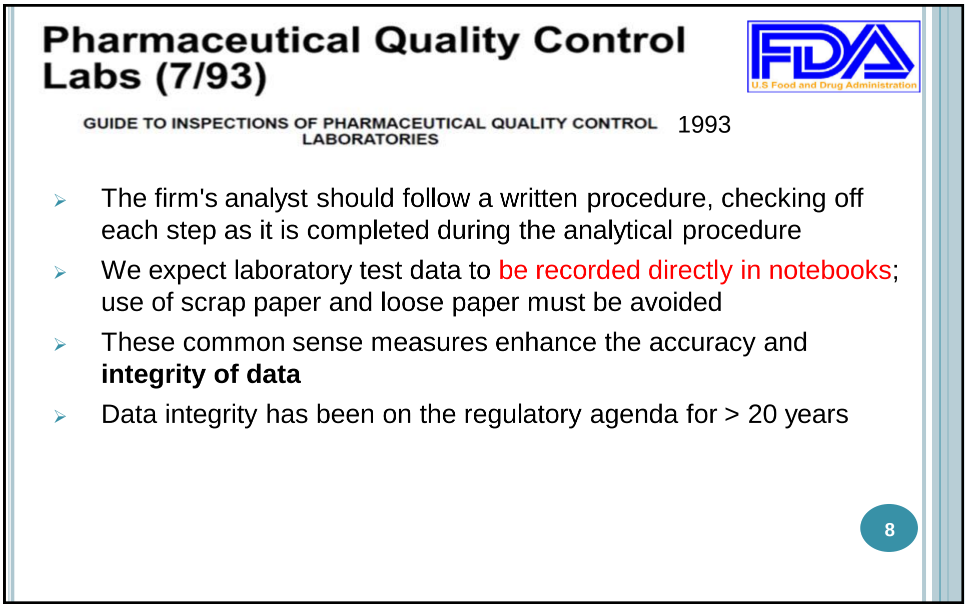
- In 1993, a major US generic drug manufacturer was prosecuted and ordered to recall millions of its tablets
- The court found these products had failed to meet quality requirements
- Barr had a history of GMP deficiencies including:
  - Misplaced records
  - Test data recorded on scrap paper
  - Failure to control manufacturing steps
  - Release of products not meeting their specifications
  - Inadequate investigation of failed products
  - Failure to validate test methods and manufacturing processes

6



USA vs. Barr Laboratories

- Established batch release criteria are absolute
- Use of outlier tests limited
  - Use banned for chemical test results
- Rules for **OOS investigations**
  - No more ‘testing into compliance’
  - OOS test results can only be overturned if laboratory error is established as the cause
- Rules on averaging test results and resampling



Pharmaceutical Quality Control Labs (7/93)

GUIDE TO INSPECTIONS OF PHARMACEUTICAL QUALITY CONTROL LABORATORIES 1993

- The firm's analyst should follow a written procedure, checking off each step as it is completed during the analytical procedure
- We expect laboratory test data to be recorded directly in notebooks; use of scrap paper and loose paper must be avoided
- These common sense measures enhance the accuracy and **integrity of data**
- Data integrity has been on the regulatory agenda for > 20 years

US FDA NEWS – AUGUST 2007

- The FDA *"is increasingly focusing on data integrity issues, including data manipulation, when conducting preapproval facility inspections"*
- This resulted from the discovery of electronic data manipulation during pre-approval inspections

FDANEWS

Simplifying Global Compliance

FDA Approves Pfizer's Mylotarg for Acute Myeloid Leukemia

Patients who received Mylotarg went longer without complications.

Read More

Recommended Products View More

Effective 483 Responses: Focus on CAPA Violations

Everyone breathes a sigh of relief when the FDA investigators depart. But if they leave a Form 483 pointing out deficiencies and noncompliances, that's when the work really starts.

Social Media Accountability for Drug and Devicemakers

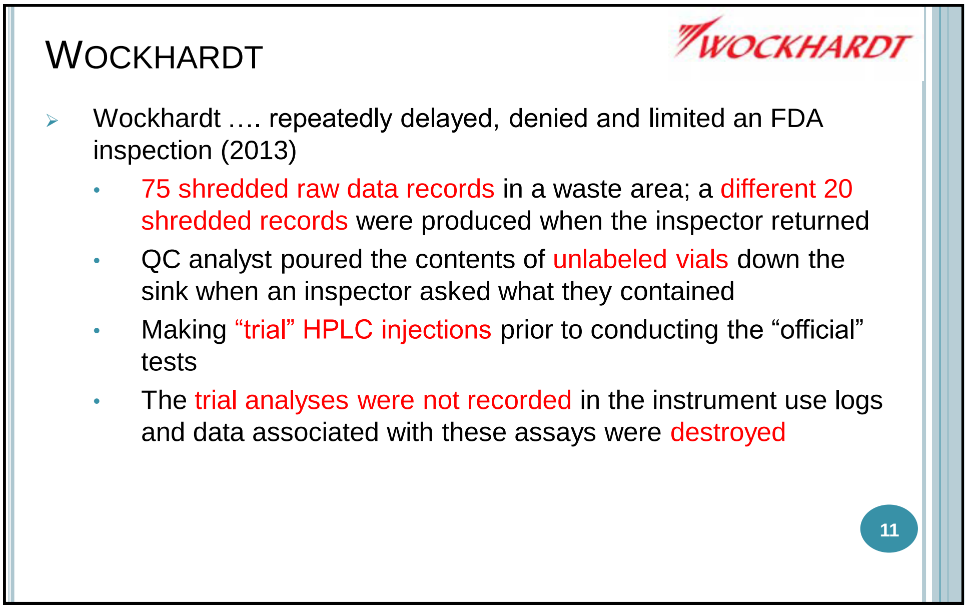
No one seems to know what the rules of social media for life sciences are, including, some might say, the FDA itself.

9

RANBAXY

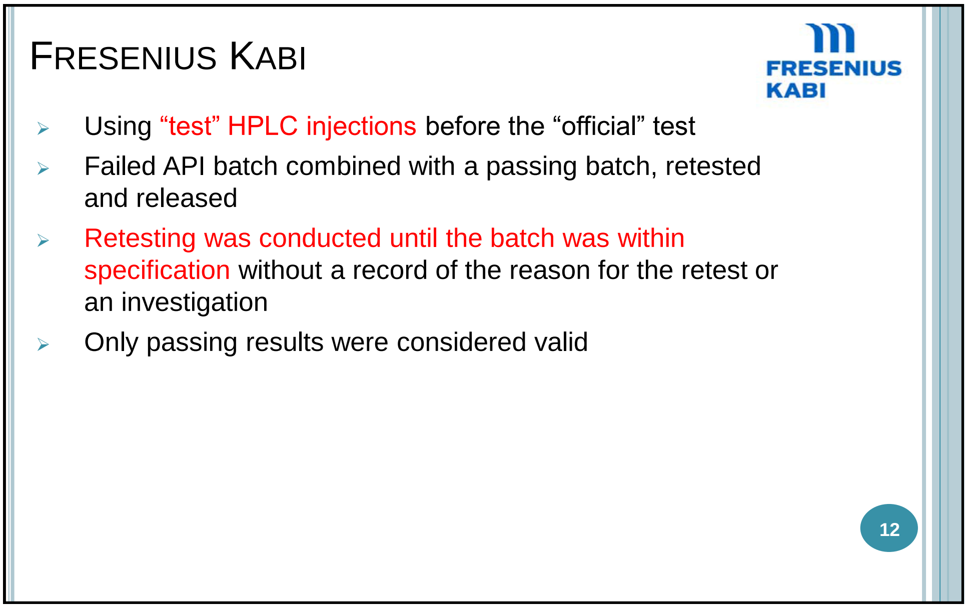
- In 2012, generics manufacturer Ranbaxy was found to have falsified data in a number of its applications
- In July 2013, the FDA issued draft guidance for industry on circumstances that constitute delaying, denying, limiting or refusing a drug inspection
  - – Food and Drug Administration Safety and Innovation Act (FDASIA) 2012

10



WOCKHARDT

- Wockhardt …. repeatedly delayed, denied and limited an FDA inspection (2013)
  - 75 shredded raw data records in a waste area; a different 20 shredded records were produced when the inspector returned
  - QC analyst poured the contents of unlabeled vials down the sink when an inspector asked what they contained
  - Making “trial” HPLC injections prior to conducting the “official” tests
  - The trial analyses were not recorded in the instrument use logs and data associated with these assays were destroyed



FRESENIUS KABI

- Using “test” HPLC injections before the “official” test
- Failed API batch combined with a passing batch, retested and released
- Retesting was conducted until the batch was within specification without a record of the reason for the retest or an investigation
- Only passing results were considered valid

FOOD AND DRUG ADMINISTRATION
COMPLIANCE PROGRAM GUIDANCE MANUAL

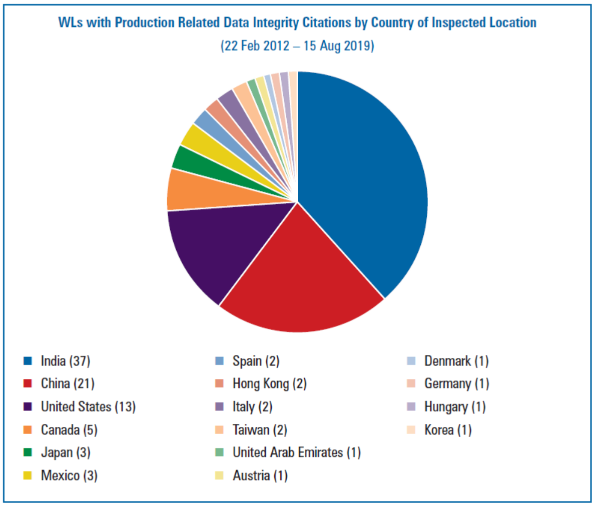
PROGRAM 7346.832

CHAPTER 46- NEW DRUG EVALUATION

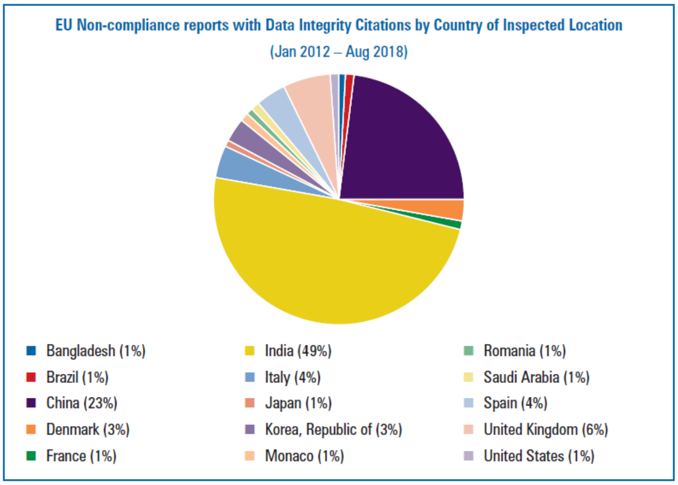
SUBJECT: PRE-APPROVAL INSPECTIONS	IMPLEMENTATION DATE 5/12/2010

- As a result of the generic drug manufacturing history … this inspectional program was significantly revised to include more emphasis on data integrity
- More than 30 individuals and nine companies admitted or were found guilty of various fraud and corruption offenses involving generic drugs
- Audit the raw data, hardcopy or electronic, to authenticate the data submitted in the CMC section of the application
- Verify that all relevant data (e.g., stability, bio batch data) were submitted in the CMC section such that CDER product reviewers can rely on the submitted data as complete and accurate

FDA WARNING LETTER



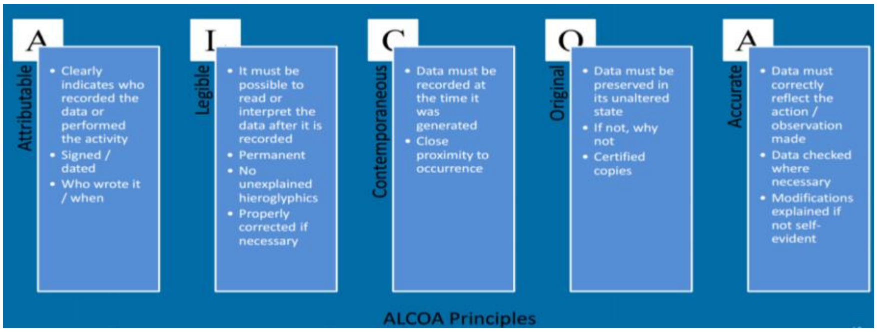
EU Non-Compliance Report



EU Non-compliance reports with Data Integrity Citations by Country of Inspected Location (Jan 2012 – Aug 2018)

Data Integrity Definitions and Requirements

GENERAL DATA INTEGRITY PRINCIPLES



A — Attributable
- Clearly indicates who recorded the data or performed the activity
- Signed / dated
- Who wrote it / when

L — Legible
- It must be possible to read or interpret the data after it is recorded
- Permanent
- No unexplained hieroglyphics
- Properly corrected if necessary

C — Contemporaneous
- Data must be recorded at the time it was generated
- Close proximity to occurrence

O — Original
- Data must be preserved in its unaltered state
- If not, why not
- Certified copies

A — Accurate
- Data must correctly reflect the action / observation made
- Data checked where necessary
- Modifications explained if not self-evident

ALCOA Principles

FDA Guide on Using Computers in Clinical Trials: ALCOA (1999)

Attributable: Who acquired the data and when

Legible: Can you read the data (e.g, handwriting, durable ink), paper and electronic

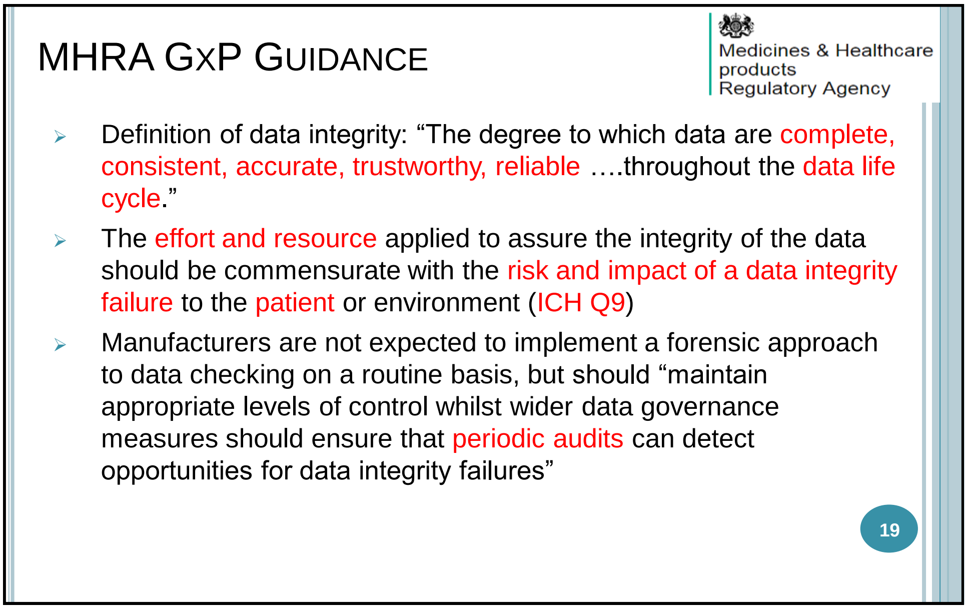
Contemporaneous: Are data recorded at the time of observation

Original: Are data presented the same as originally recorded

Accurate: Are data correct throughout the entire lifecycle

ALCOA +

- Complete: All information that would be **critical** to recreating an event is important when trying to understand the event.
- Consistent: **Good Documentation Practices** should be applied throughout any process
- Enduring: Part of ensuring records are available is making sure they exist for the **entire period** during which they might be needed.
- Available: Records must be available for review at any time during the required **retention period**

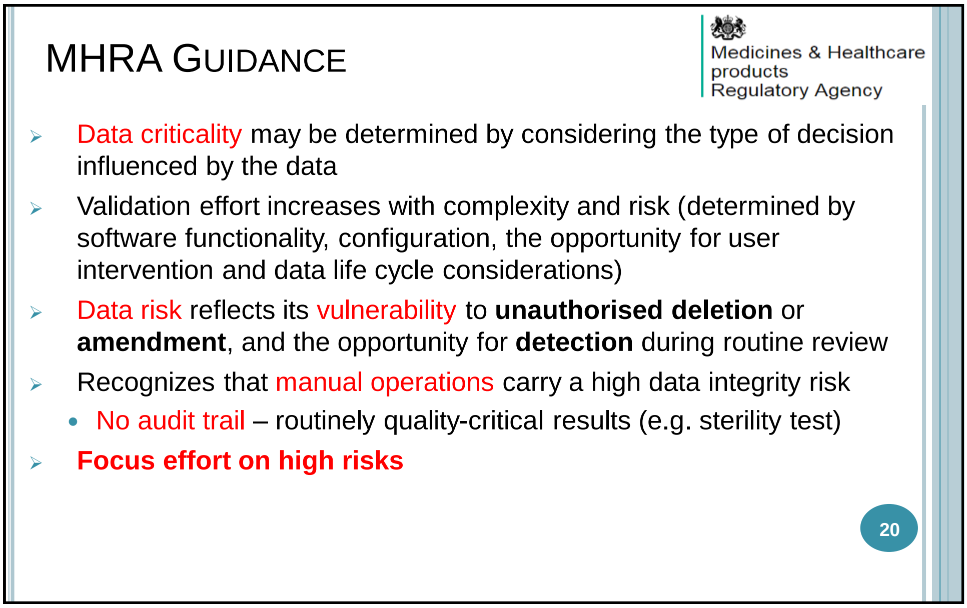


MHRA GxP Guidance

Medicines & Healthcare products Regulatory Agency

- Definition of data integrity: "The degree to which data are complete, consistent, accurate, trustworthy, reliable ….throughout the data life cycle."
- The effort and resource applied to assure the integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment (ICH Q9)
- Manufacturers are not expected to implement a forensic approach to data checking on a routine basis, but should "maintain appropriate levels of control whilst wider data governance measures should ensure that periodic audits can detect opportunities for data integrity failures"

19

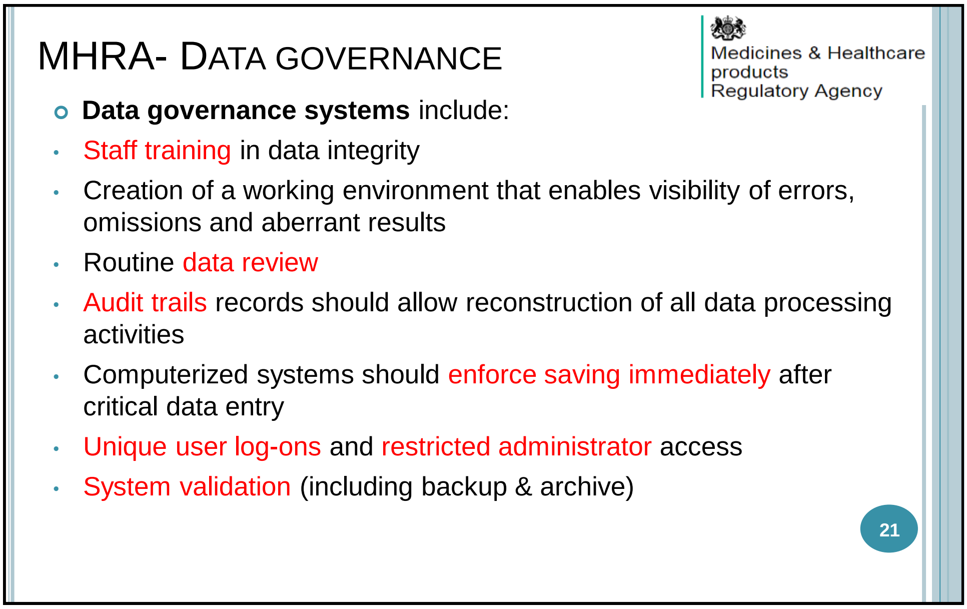


MHRA Guidance

Medicines & Healthcare products Regulatory Agency

- Data criticality may be determined by considering the type of decision influenced by the data
- Validation effort increases with complexity and risk (determined by software functionality, configuration, the opportunity for user intervention and data life cycle considerations)
- Data risk reflects its vulnerability to **unauthorised deletion** or **amendment**, and the opportunity for **detection** during routine review
- Recognizes that manual operations carry a high data integrity risk
  - No audit trail – routinely quality-critical results (e.g. sterility test)
- **Focus effort on high risks**

20

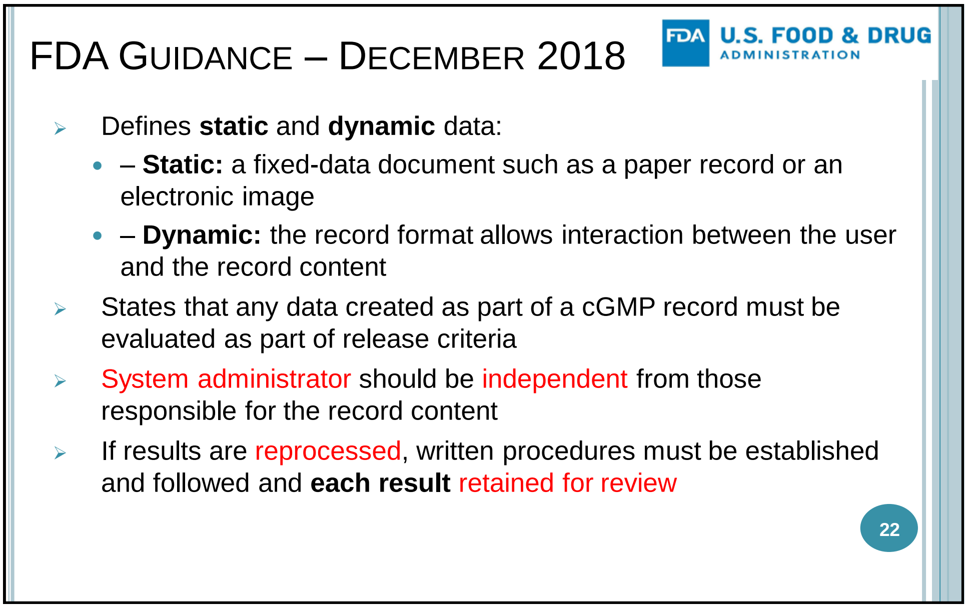


MHRA- Data Governance

Medicines & Healthcare products Regulatory Agency

- **Data governance systems** include:
- Staff training in data integrity
- Creation of a working environment that enables visibility of errors, omissions and aberrant results
- Routine data review
- Audit trails records should allow reconstruction of all data processing activities
- Computerized systems should enforce saving immediately after critical data entry
- Unique user log-ons and restricted administrator access
- System validation (including backup & archive)

21

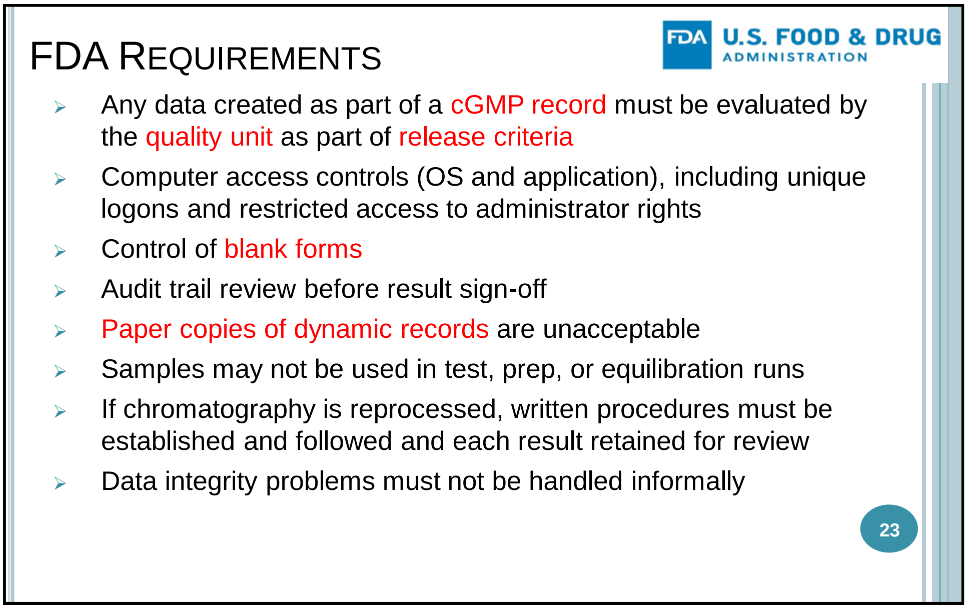


FDA Guidance – December 2018

FDA U.S. FOOD & DRUG ADMINISTRATION

- Defines **static** and **dynamic** data:
  - – **Static:** a fixed-data document such as a paper record or an electronic image
  - – **Dynamic:** the record format allows interaction between the user and the record content
- States that any data created as part of a cGMP record must be evaluated as part of release criteria
- System administrator should be independent from those responsible for the record content
- If results are reprocessed, written procedures must be established and followed and **each result** retained for review

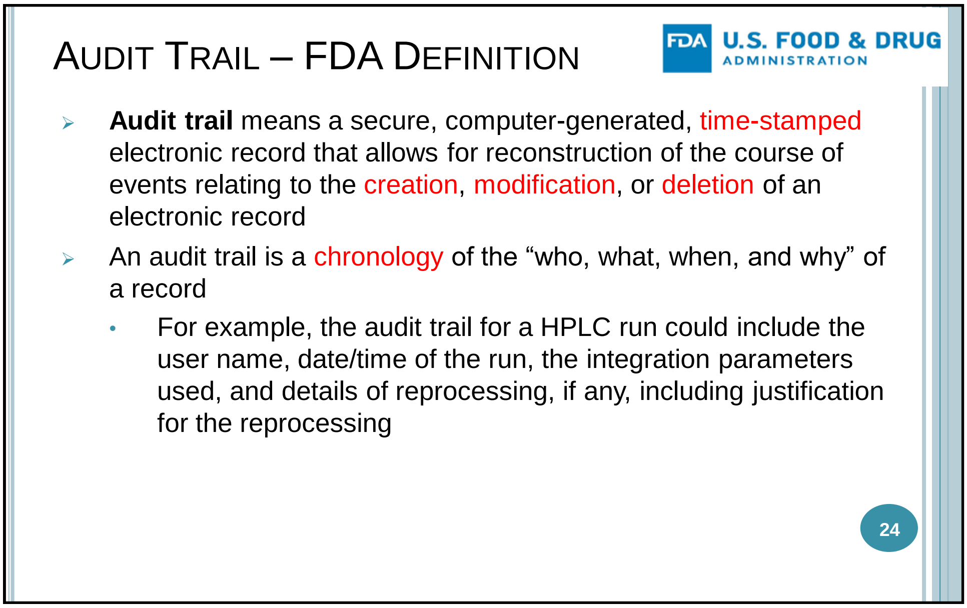
22



FDA Requirements

FDA U.S. FOOD & DRUG ADMINISTRATION

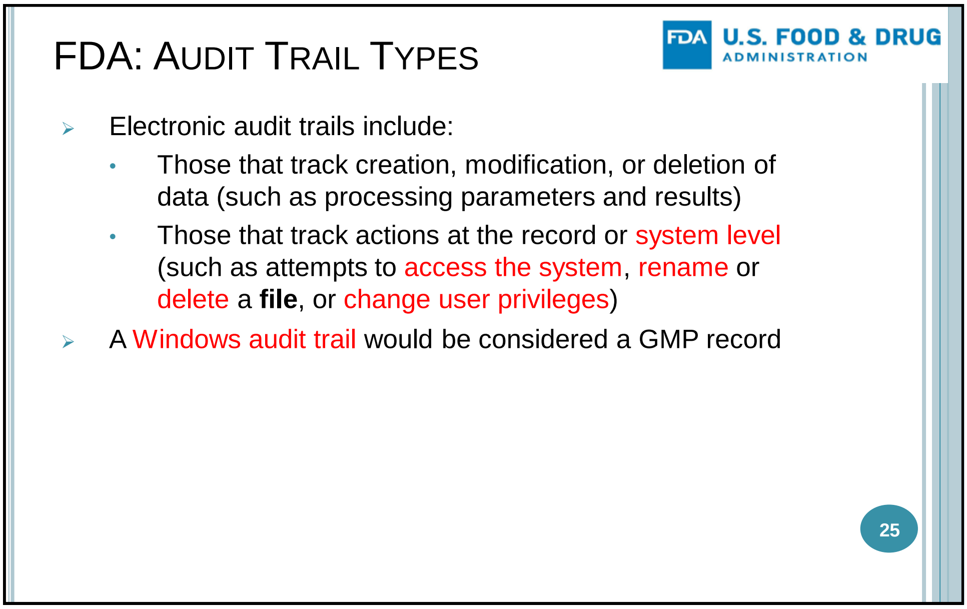
- Any data created as part of a cGMP record must be evaluated by the quality unit as part of release criteria
- Computer access controls (OS and application), including unique logons and restricted access to administrator rights
- Control of blank forms
- Audit trail review before result sign-off
- Paper copies of dynamic records are unacceptable
- Samples may not be used in test, prep, or equilibration runs
- If chromatography is reprocessed, written procedures must be established and followed and each result retained for review
- Data integrity problems must not be handled informally



Audit Trail – FDA Definition

FDA U.S. FOOD & DRUG ADMINISTRATION

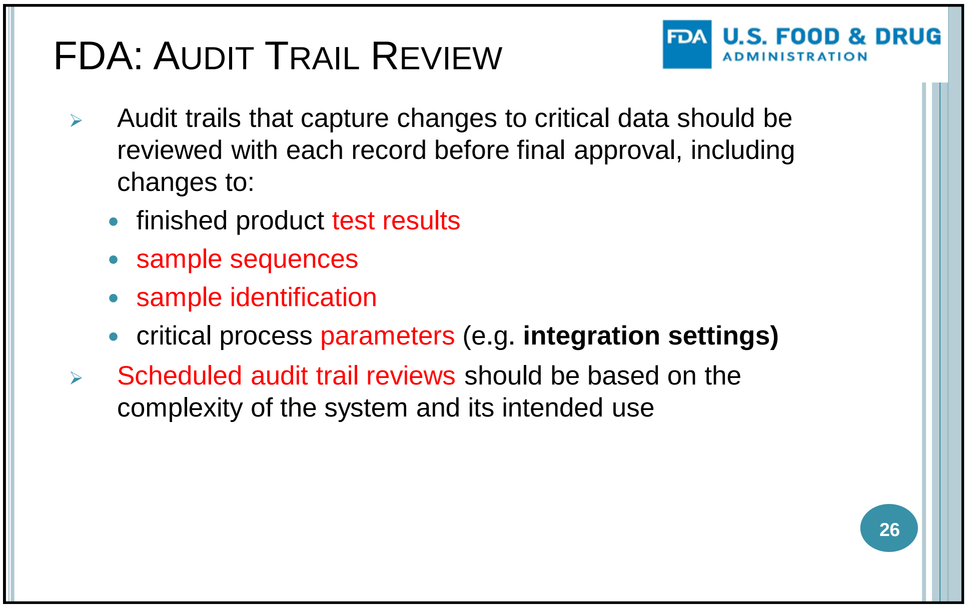
- **Audit trail** means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record
- An audit trail is a chronology of the “who, what, when, and why” of a record
  - For example, the audit trail for a HPLC run could include the user name, date/time of the run, the integration parameters used, and details of reprocessing, if any, including justification for the reprocessing



FDA: Audit Trail Types

U.S. FOOD & DRUG ADMINISTRATION

- Electronic audit trails include:
  - Those that track creation, modification, or deletion of data (such as processing parameters and results)
  - Those that track actions at the record or system level (such as attempts to access the system, rename or delete a **file**, or change user privileges)
- A Windows audit trail would be considered a GMP record



FDA: Audit Trail Review

U.S. FOOD & DRUG ADMINISTRATION

- Audit trails that capture changes to critical data should be reviewed with each record before final approval, including changes to:
  - finished product test results
  - sample sequences
  - sample identification
  - critical process parameters (e.g. **integration settings)**
- Scheduled audit trail reviews should be based on the complexity of the system and its intended use

EMA Guidance – August 2016

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

- Posted in Q&A format on the EMA's web site
- Encourages a risk-based approach (similar to MHRA) and covers:
  - Evaluation of data risk/criticality
  - Defines a life cycle approach to data control
  - Suggests that organizations prepare a document summarizing their approach to data governance
  - Requires control of blank forms/templates
  - Requires electronic review of electronic data
  - Coverage of data integrity during internal audit
  - Requirement to check data integrity practices at contractors' sites

WHO Annex 5: Guidance on good data and record management practices (2016)

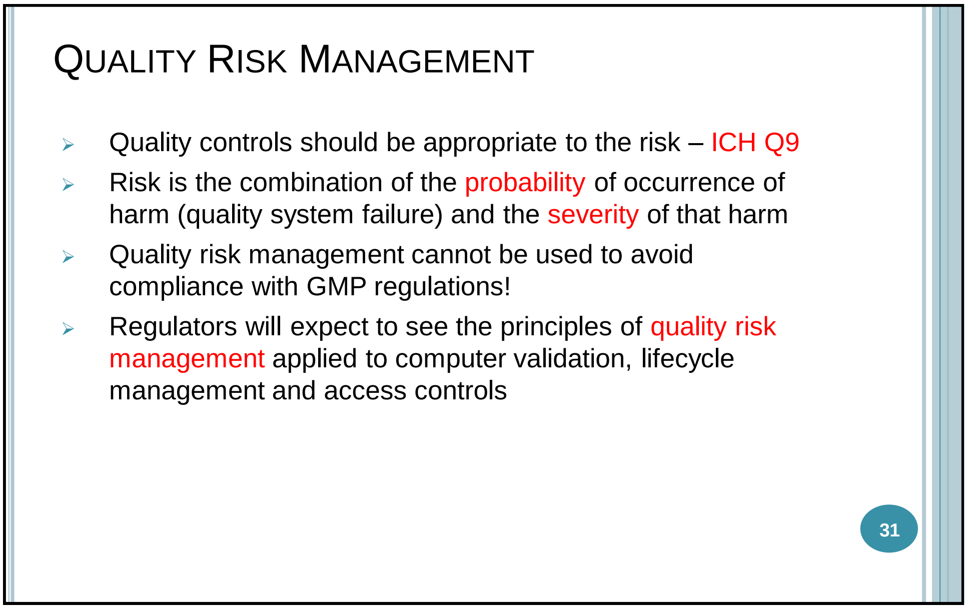
World Health Organization

- Principles of data integrity (including data governance)
- Quality risk management to ensure good data management
- Management governance and quality audits
- Contracted organizations, suppliers and service providers
- Training in good data and record management
- Good documentation practices
- Designing and validating systems to assure data quality and
- reliability
- Managing data and records throughout the data life cycle

PIC/S: GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS (PI 041-1, DRAFT 3; 2018)

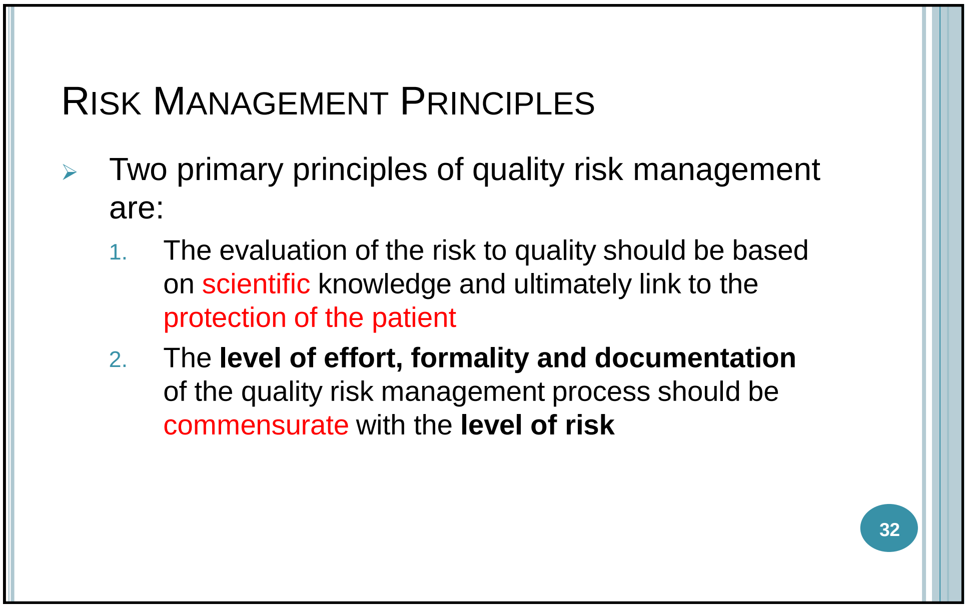
- Adopts a risk-based approach
- Intended as a guide for regulators
- Follows MHRA approach closely
  - MHRA was co-chair of PIC/S data integrity working group together with the Australian regulatory agency (TGA)

DATA INTEGRITY RISK ASSESSMENT



Quality Risk Management

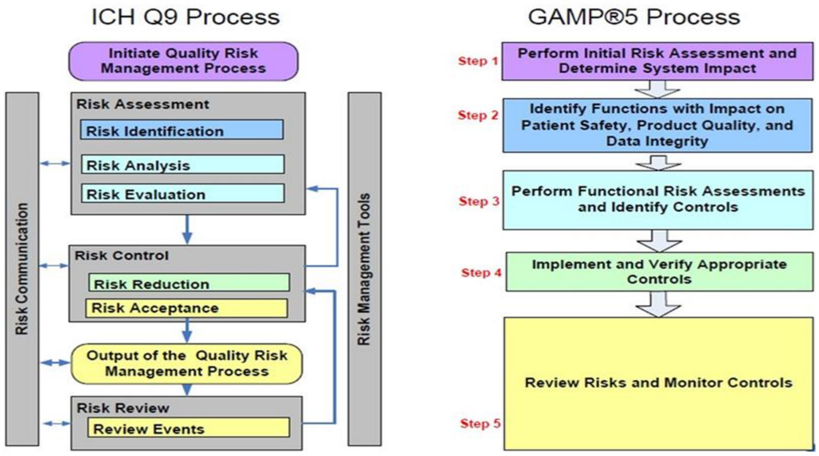
- Quality controls should be appropriate to the risk – ICH Q9
- Risk is the combination of the probability of occurrence of harm (quality system failure) and the severity of that harm
- Quality risk management cannot be used to avoid compliance with GMP regulations!
- Regulators will expect to see the principles of quality risk management applied to computer validation, lifecycle management and access controls



Risk Management Principles

- Two primary principles of quality risk management are:
  1. The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient
  2. The **level of effort, formality and documentation** of the quality risk management process should be commensurate with the **level of risk**

ICH Q9 vs. GAMP 5



ICH Q9 Process

Initiate Quality Risk Management Process

Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation

Risk Control
- Risk Reduction
- Risk Acceptance

Output of the Quality Risk Management Process

Risk Review
- Review Events

Risk Communication

Risk Management Tools

GAMP®5 Process

Step 1 Perform Initial Risk Assessment and Determine System Impact

Step 2 Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity

Step 3 Perform Functional Risk Assessments and Identify Controls

Step 4 Implement and Verify Appropriate Controls

Step 5 Review Risks and Monitor Controls

33

Data Integrity Controls

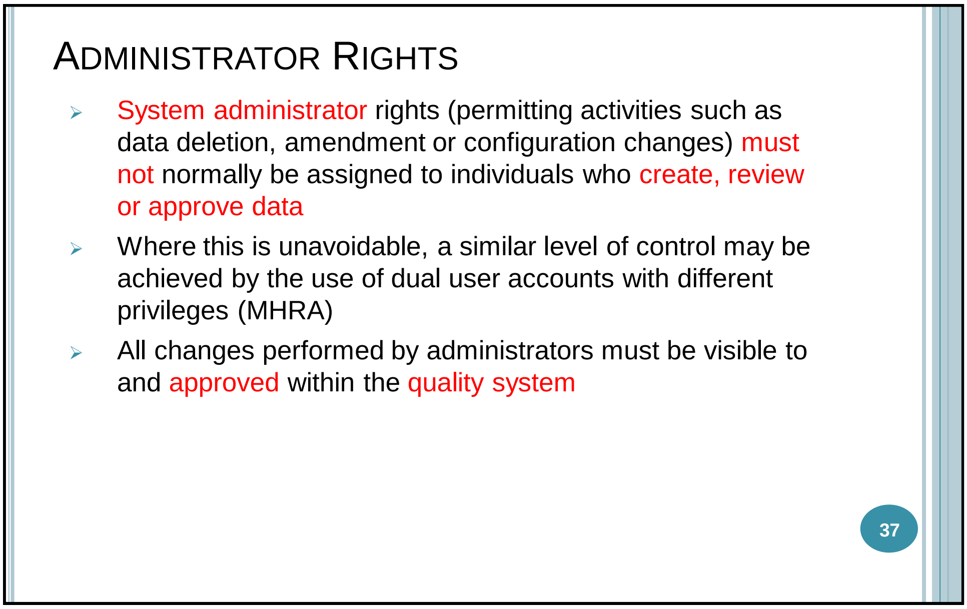
34

DATA INTEGRITY RISKS

Manual operations carry the greatest risk

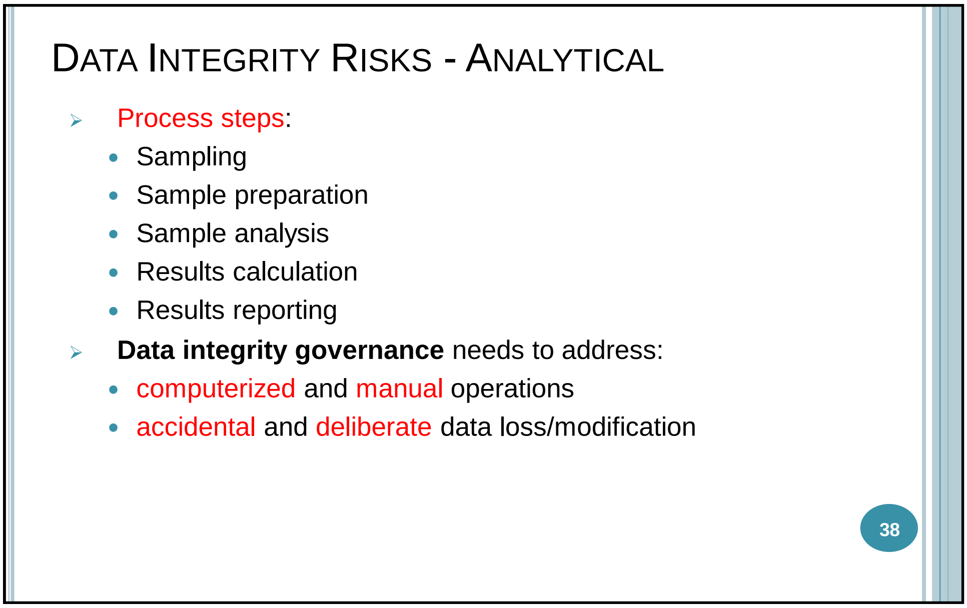
DATA INTEGRITY CONTROLS

- Access to clocks for recording timed events (e.g. computer and balance printer time/date settings)
- Data written directly onto final record
- Control over blank paper templates for data recording
- User access rights which prevent data amendment
- Automated data capture or printers (e.g. for balances)
- Access to raw data for staff performing data checking



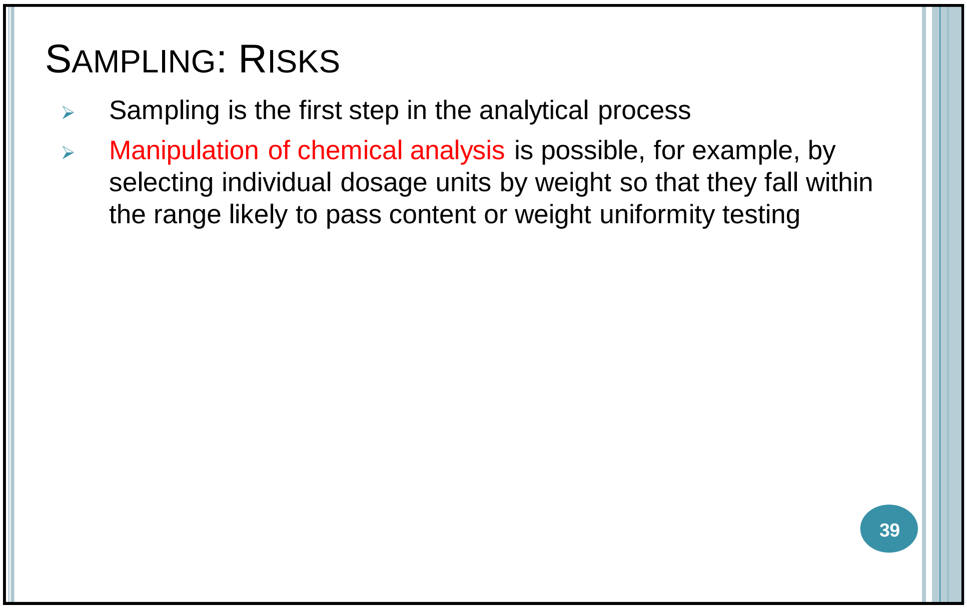
ADMINISTRATOR RIGHTS

- System administrator rights (permitting activities such as data deletion, amendment or configuration changes) must not normally be assigned to individuals who create, review or approve data
- Where this is unavoidable, a similar level of control may be achieved by the use of dual user accounts with different privileges (MHRA)
- All changes performed by administrators must be visible to and approved within the quality system



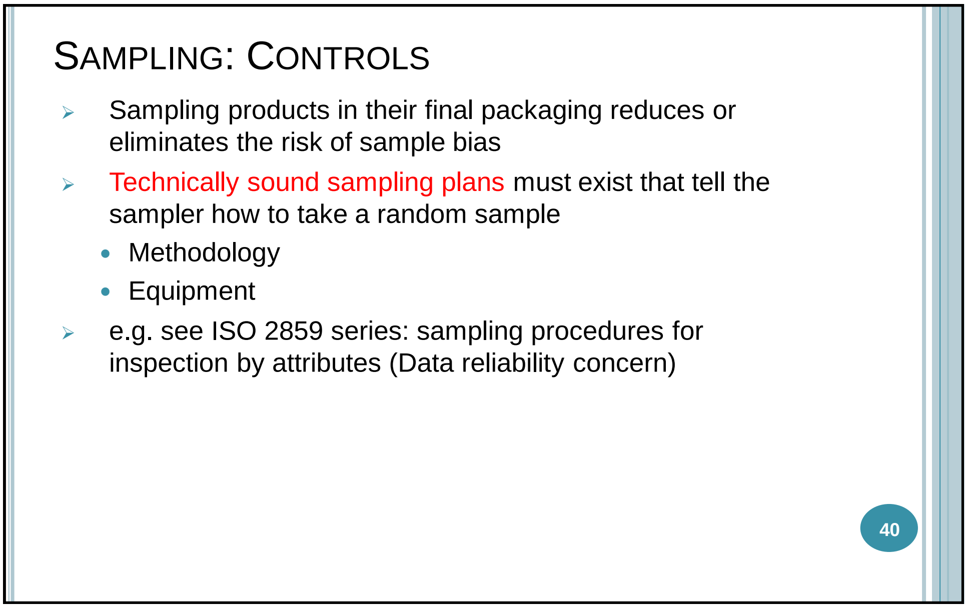
DATA INTEGRITY RISKS - ANALYTICAL

- Process steps:
  - Sampling
  - Sample preparation
  - Sample analysis
  - Results calculation
  - Results reporting
- **Data integrity governance** needs to address:
  - computerized and manual operations
  - accidental and deliberate data loss/modification



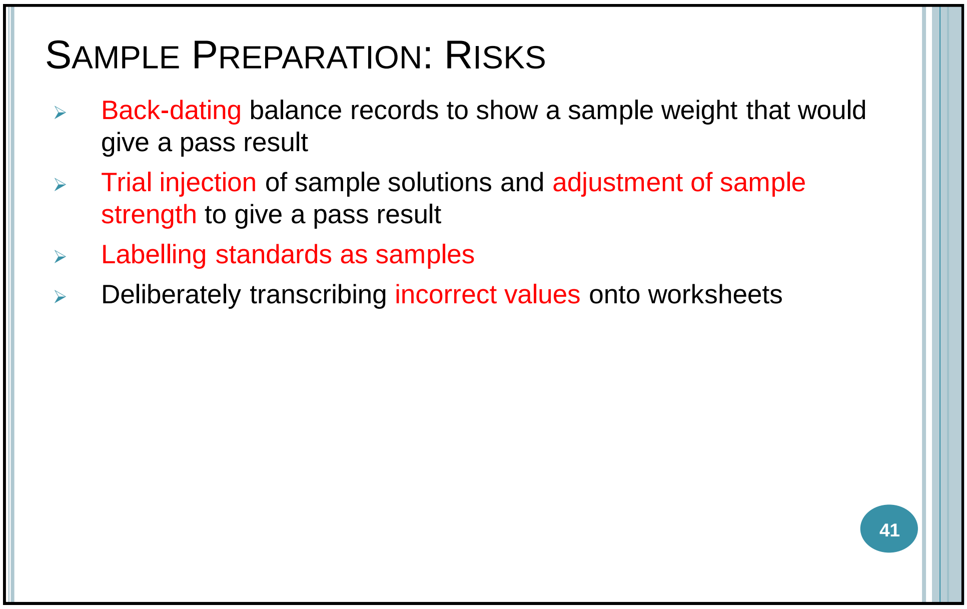
SAMPLING: RISKS

- Sampling is the first step in the analytical process
- Manipulation of chemical analysis is possible, for example, by selecting individual dosage units by weight so that they fall within the range likely to pass content or weight uniformity testing



SAMPLING: CONTROLS

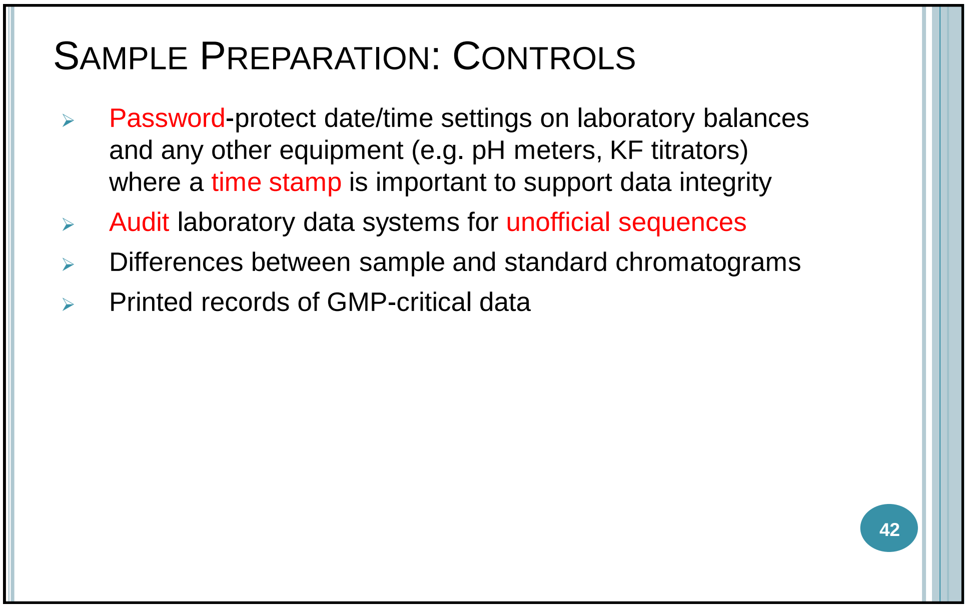
- Sampling products in their final packaging reduces or eliminates the risk of sample bias
- Technically sound sampling plans must exist that tell the sampler how to take a random sample
  - Methodology
  - Equipment
- e.g. see ISO 2859 series: sampling procedures for inspection by attributes (Data reliability concern)



Sample Preparation: Risks

- Back-dating balance records to show a sample weight that would give a pass result
- Trial injection of sample solutions and adjustment of sample strength to give a pass result
- Labelling standards as samples
- Deliberately transcribing incorrect values onto worksheets

41



Sample Preparation: Controls

- Password-protect date/time settings on laboratory balances and any other equipment (e.g. pH meters, KF titrators) where a time stamp is important to support data integrity
- Audit laboratory data systems for unofficial sequences
- Differences between sample and standard chromatograms
- Printed records of GMP-critical data

42

EXAMPLE: LABORATORY BALANCE

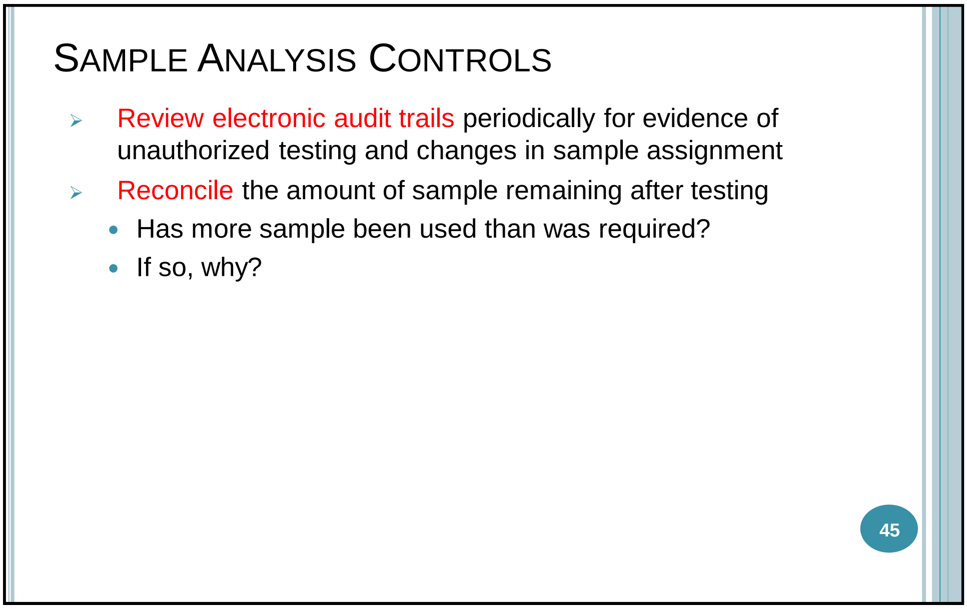
- Electronic record with full audit control
- Manual transcription can be avoided

- Paper record with password
- Protected time/date stamp
- Different levels of user access may be configured

Images & information courtesy of Mettler Toledo

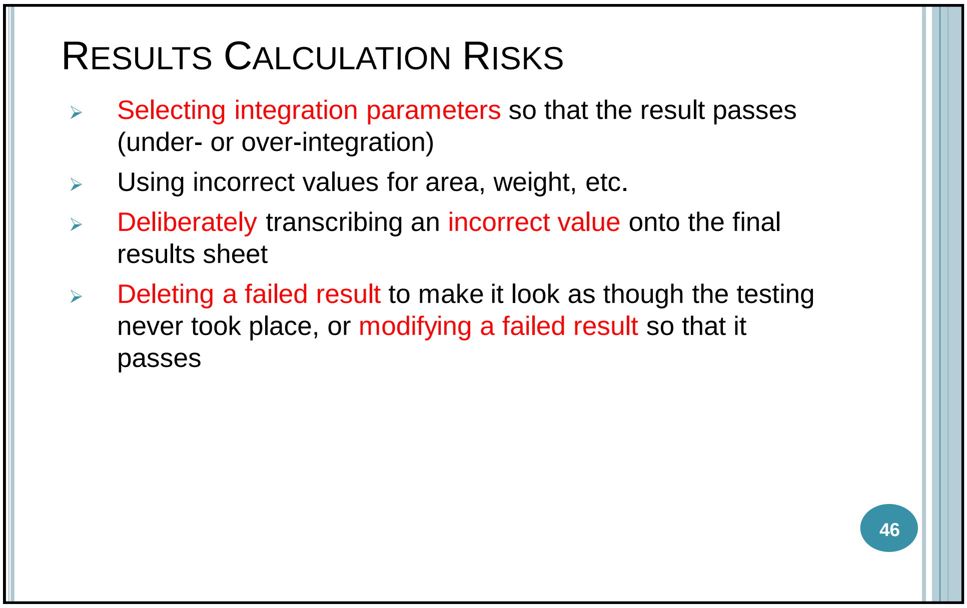
SAMPLE ANALYSIS RISKS

- Unauthorized retesting of failed samples
- Altering the assignment of an injection (e.g. ‘standard’ or ‘sample’ to ‘equilibration’ post-run)
- Deliberately testing the wrong sample (e.g. one that has previously passed)



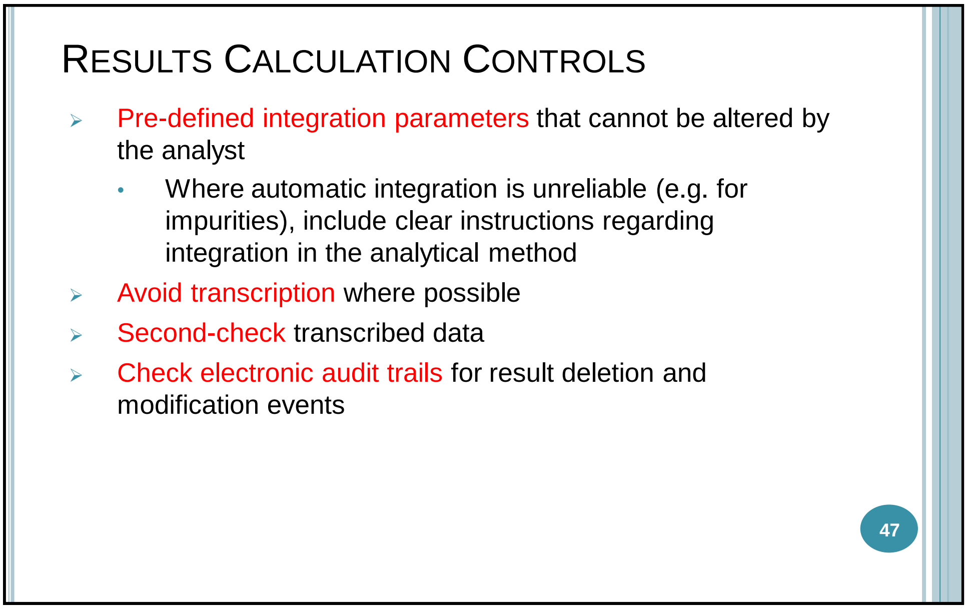
Sample Analysis Controls

- Review electronic audit trails periodically for evidence of unauthorized testing and changes in sample assignment
- Reconcile the amount of sample remaining after testing
  - Has more sample been used than was required?
  - If so, why?



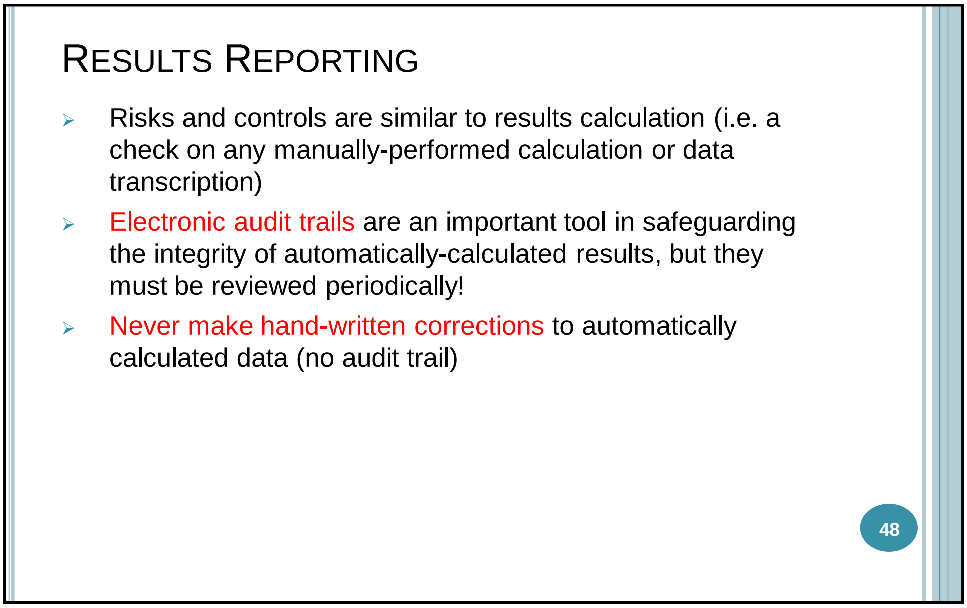
Results Calculation Risks

- Selecting integration parameters so that the result passes (under- or over-integration)
- Using incorrect values for area, weight, etc.
- Deliberately transcribing an incorrect value onto the final results sheet
- Deleting a failed result to make it look as though the testing never took place, or modifying a failed result so that it passes



Results Calculation Controls

- Pre-defined integration parameters that cannot be altered by the analyst
  - Where automatic integration is unreliable (e.g. for impurities), include clear instructions regarding integration in the analytical method
- Avoid transcription where possible
- Second-check transcribed data
- Check electronic audit trails for result deletion and modification events



Results Reporting

- Risks and controls are similar to results calculation (i.e. a check on any manually-performed calculation or data transcription)
- Electronic audit trails are an important tool in safeguarding the integrity of automatically-calculated results, but they must be reviewed periodically!
- Never make hand-written corrections to automatically calculated data (no audit trail)

The Human Factor

Improve quality of the product !!
As I reported, We tried a lot of methods. But not yet…
You must think how to finish !!
Too late !! You must finish now !
How can we finish ? We need time and budget for research.
We can't proceed. Only way is falsifying the data of quality…
REPORT
BAD
REPORT
GOOD

- A good quality culture is critical
  - Mistakes must not be hidden – avoid blame

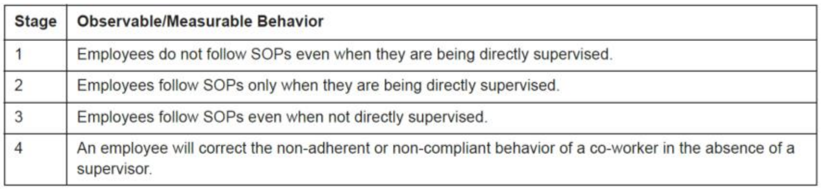
Quality Culture

- Management should create a culture in which staff can communicate failures and mistakes, including data reliability issues, so that corrective and preventive actions can be taken
- This includes ensuring adequate information flow between staff at all levels
- Senior management should discourage any management practices that might inhibit the reporting of such issues, e.g. hierarchies and blame cultures

Quality Culture

- The proper use of risk controls should be described in SOPs. Administrative procedures should ensure that personnel understand the practical implications of the risks set out in the SOPs.

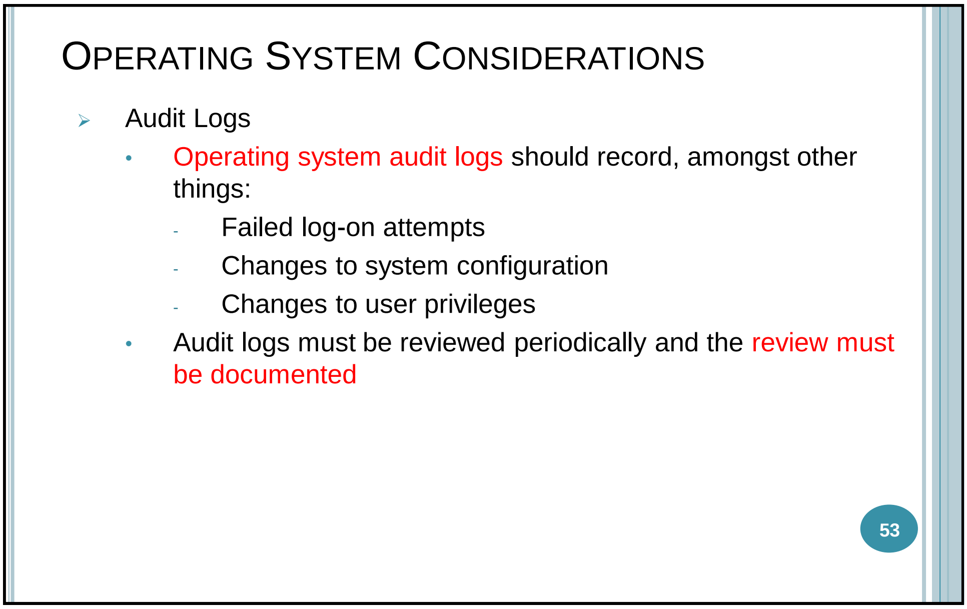
Quality Culture of an Organization



Stage	Observable/Measurable Behavior
1	Employees do not follow SOPs even when they are being directly supervised.
2	Employees follow SOPs only when they are being directly supervised.
3	Employees follow SOPs even when not directly supervised.
4	An employee will correct the non-adherent or non-compliant behavior of a co-worker in the absence of a supervisor.

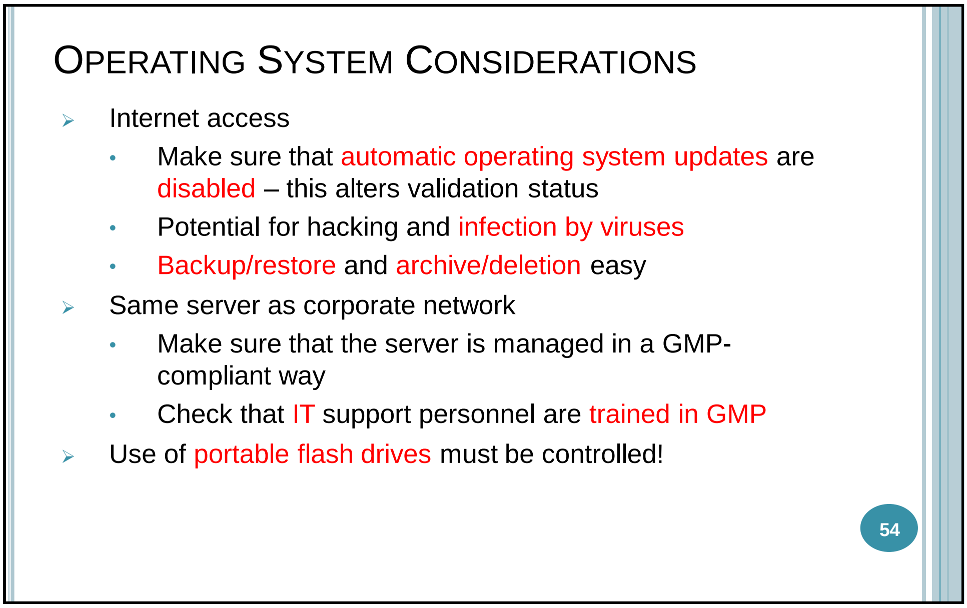
ISPE Risk-MaPP Volume 7

Computerized Systems



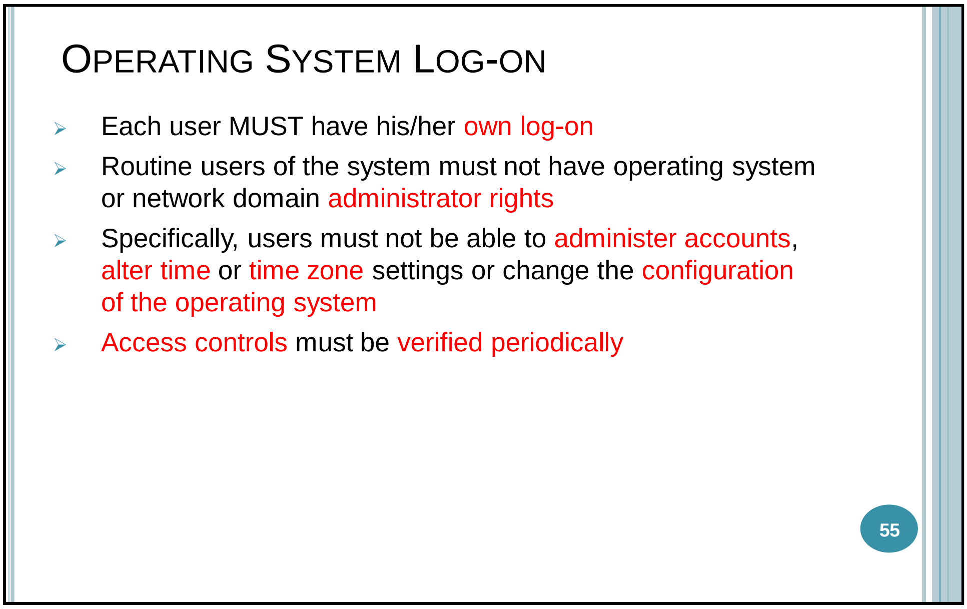
Operating System Considerations

- Audit Logs
  - Operating system audit logs should record, amongst other things:
    - Failed log-on attempts
    - Changes to system configuration
    - Changes to user privileges
  - Audit logs must be reviewed periodically and the review must be documented



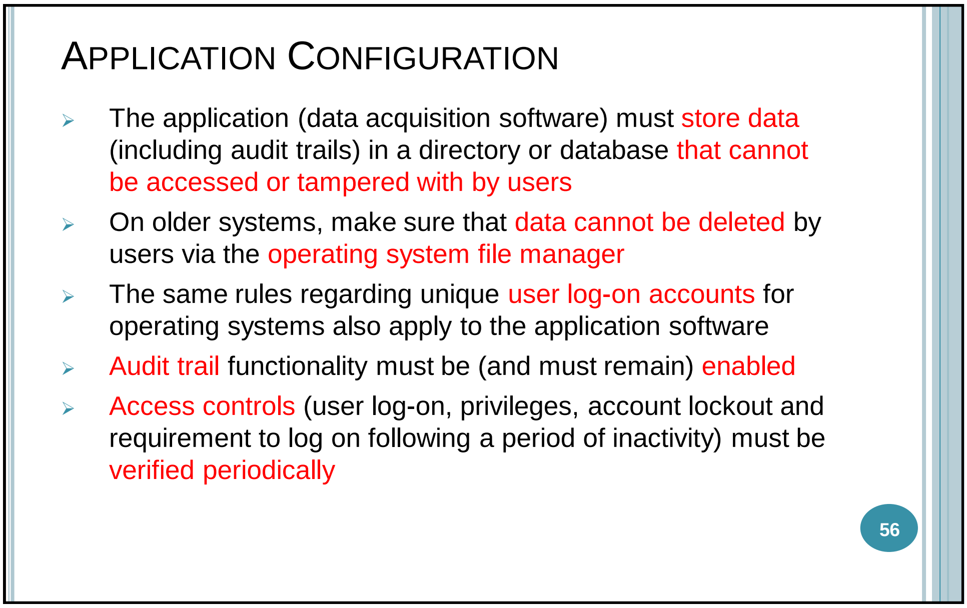
Operating System Considerations

- Internet access
  - Make sure that automatic operating system updates are disabled – this alters validation status
  - Potential for hacking and infection by viruses
  - Backup/restore and archive/deletion easy
- Same server as corporate network
  - Make sure that the server is managed in a GMP-compliant way
  - Check that IT support personnel are trained in GMP
- Use of portable flash drives must be controlled!



Operating System Log-on

- Each user MUST have his/her own log-on
- Routine users of the system must not have operating system or network domain administrator rights
- Specifically, users must not be able to administer accounts, alter time or time zone settings or change the configuration of the operating system
- Access controls must be verified periodically



Application Configuration

- The application (data acquisition software) must store data (including audit trails) in a directory or database that cannot be accessed or tampered with by users
- On older systems, make sure that data cannot be deleted by users via the operating system file manager
- The same rules regarding unique user log-on accounts for operating systems also apply to the application software
- Audit trail functionality must be (and must remain) enabled
- Access controls (user log-on, privileges, account lockout and requirement to log on following a period of inactivity) must be verified periodically

CHROMATOGRAPHY DATA SYSTEMS

- Metadata (acquisition and processing parameters) must be stored with the original raw data file
- Data systems must be audited periodically for the presence of unauthorized sequences
  - Such sequences have been used in the past to make a trial injection of a sample to establish whether or not it is likely to meet specification during subsequent “official” testing
- The injection type (calibration standard, sample, blank or system suitability) must be clearly identified
- Corrections to processed data must be made via the data system, not by hand (no audit trail)

DATA BACKUP AND RESTORE

- Backup is the process of copying electronic records to protect against loss of integrity or availability of the original record
- Written, verified procedures must be in place describing routine backup (and restoration following failure)
- Backup frequency should be risk-based
- Backup log must include details of the media used for storage

59

Questions?

60