



Audit Trail and its Review

Roberto Bertini, Executive Consultant & Operations Manager, PQE Group 

Audit Trail:

A secure, computer-generated, time-stamped log that independently records the date and time of user entries and actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Audit trail must capture the old value, the new value, who created/changed/deleted the record, date and time when it has been done, and the reason for the change (if applicable).

Audit Trails include:

- Operative Audit Trails that track creation, modification, or deletion of process data (such as processing parameters and results)
- Administrative Audit Trails (or System Audit Trail) that track actions at the record or system level (such as attempts to access the system, rename or delete a file, changes to user profiles).

EU GMP Annex 11 – June 2011

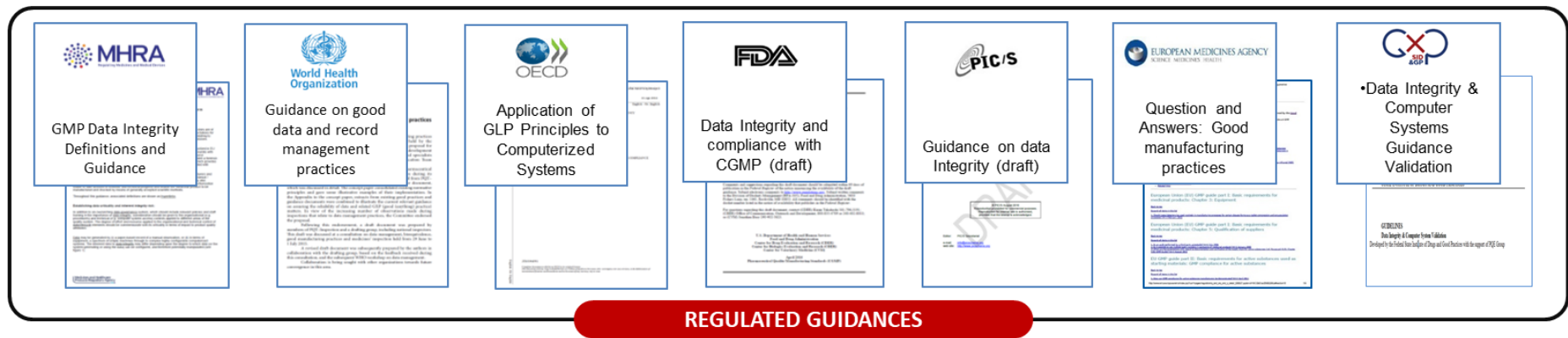
9 - **Audit Trails** - Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. **Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.**

US FDA 21 CFR Part 11 – March 1997

§ 11.10 Controls for closed systems - Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ **procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records**, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

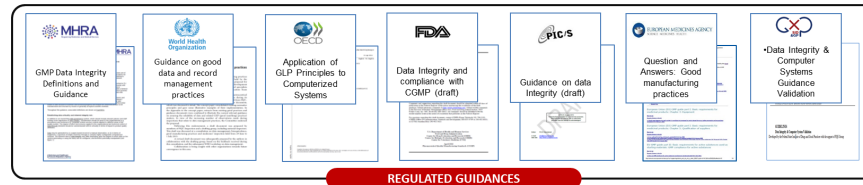
[...] **(e) Use of secure, computer-generated, time-stamped audit trails** to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying

- Status
 - Increase in number and severity of DI findings by almost every Regulated Agency
 - Impact to public health
 - Increased focus
- Almost every leading Regulated Agencies has issued some guidances to clarify expectations related to Data Integrity

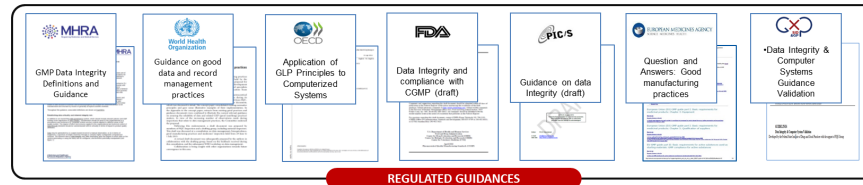


The image displays seven regulatory guidance documents from various agencies, arranged horizontally. Each document is represented by a white box with a blue border, containing the agency logo and the title of the guidance. Below the titles are smaller, partially visible images of the document pages. A red banner at the bottom of the row contains the text "REGULATED GUIDANCES".

Agency	Guidance Title
MHRA	GMP Data Integrity Definitions and Guidance
World Health Organization	Guidance on good data and record management practices
OECD	Application of GLP Principles to Computerized Systems
FDA	Data Integrity and compliance with CGMP (draft)
PIC/S	Guidance on data Integrity (draft)
EUROPEAN MEDICINES AGENCY	Question and Answers: Good manufacturing practices
GAMP	Data Integrity & Computer Systems Guidance Validation



- GxP relevant Computerized Systems managing Regulated Electronic Records should be provided with secure, computer-generated **Audit Trails suitable for regular review**
- Its recommended to implement a **risk based approach** to audit trail review which considers the **complexity** of the system and its **intended use**
- Audit trails are considered part of the associated records. Audit Trail Review should be executed by the person who is **responsible for the review of Data the Audit Trail refers to**
- Audit trails subject to regular review should include, but are not limited to, the following: the change history of finished product test results, changes to sample run sequences, changes to sample identification, and changes to critical process parameters.

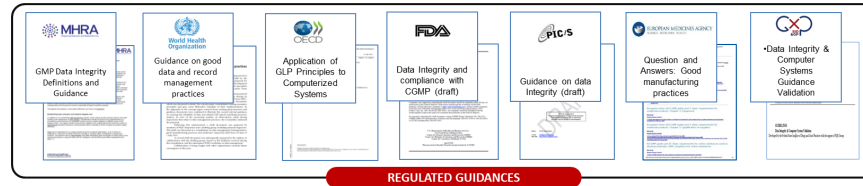


- The Audit Trail Review should be executed according to:
 - company **procedures** which define **frequency** and **extent** of the review.
 - pre-approved instructions describing the **specific controls** to be addressed by the review and related **acceptance criteria**.

- Validated **exception reports** providing clear evidence of occurred events and changes to ERs can be used to support the Audit Trail Review process.

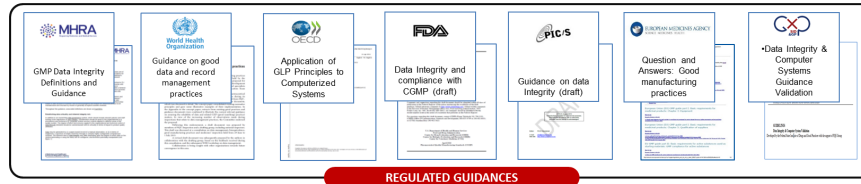
- The **results** of the review should be **documented** according to approved procedures.

- In case of observed non conformities, an investigation shall be initiated and managed according to the companies applicable procedures.



The Operative Audit Trail review should be focused as a minimum upon:

- Changes to process/test parameters
- Changes to data processing parameters
- Deletion of Process Data (e.g. Injections, results)
- Suspicious patterns (e.g. repeated analysis or reprocessing without documented rationale to support the repetition)



The Administrative Audit Trail review should be focused as a minimum upon:

- List of active user accounts
- User Access log, including failed attempts
- Changes to user roles configuration
- Changes to other configuration settings of the software application

An effective risk based approach should consider:

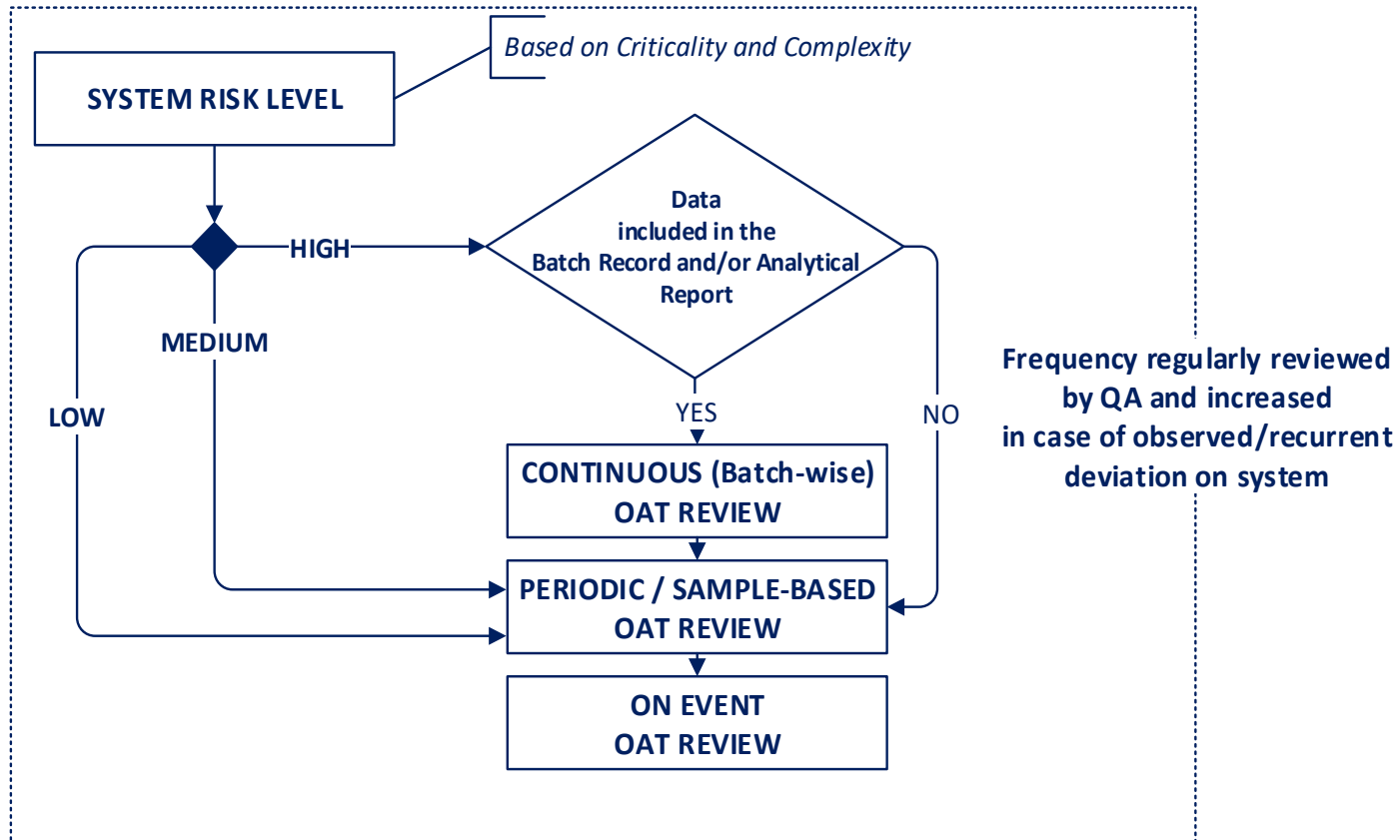
- **Data criticality**, that is determined by the system Intended Use and consequent data impact to decision making and product quality
- **Data Risk** (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes). Risk to data integrity may differ depending upon the system generating or using the data and upon the degree to which data can be configured, and therefore potentially manipulated. Thus, the necessary level of effort for the audit trail review (along with audit trail functionalities) should be associated with system complexity

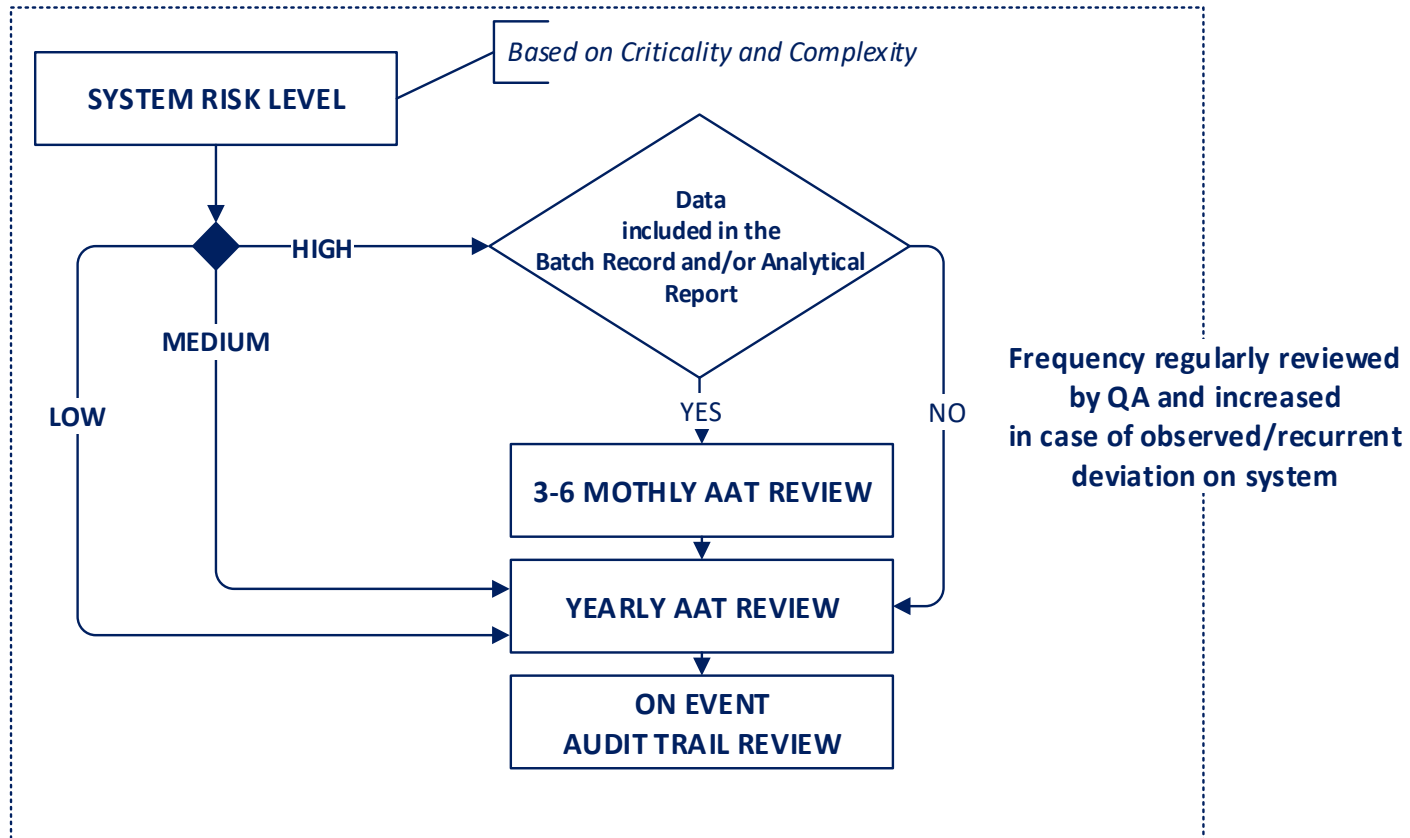
Effort to be put into the Audit Trail Review process can be defined by evaluation of the **System Risk Level**:

- **System Criticality** - determined by **criticality of records** maintained by the system itself to patient safety/product quality
- **System Complexity** - based on the **degree to which data can be configured** and therefore potentially manipulated

SYSTEM COMPLEXITY	HIGH	LOW	MEDIUM	HIGH
	MEDIUM	LOW	MEDIUM	HIGH
	LOW	LOW	MEDIUM	HIGH
		LOW	MEDIUM	HIGH
		SYSTEM CRITICALITY		

Evaluation of the System Risk Level

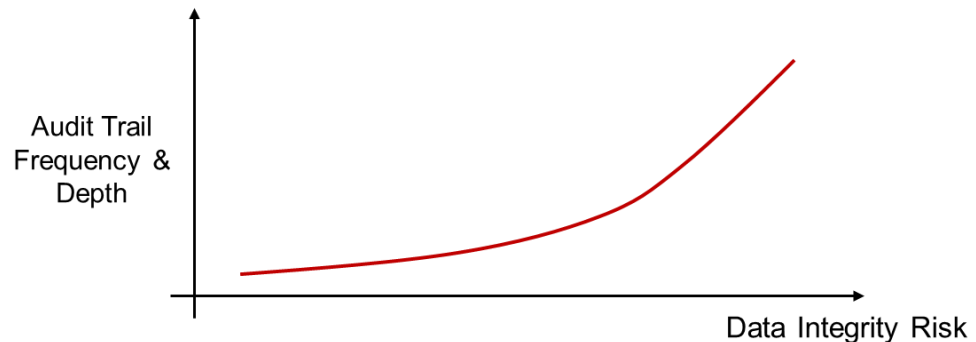




- Audit trails functionality of a system, when available, does not meet all necessary requirements of audit trails
- Audit Trail of some systems logs every event that has occurred
- Audit Trail review requires interruption of the workflow
- Multiple audit trails within the system

The Audit Trail Review may have a deep impact on routine operations since it requires resources and may affect the general release lead time

- Commensurate the Audit Trail frequency and depth of verifications with the risk associated to the Record



- Include necessary requirements for Audit Trail and Audit Trail Review (including those related to suitable tools for a timely and effective AT review) in the User Requirements of related Computerized System and ensure all requirements are properly addressed throughout the Validation Life-Cycle



www.pqegroup.com
info@pqegroup.com

Acknowledgements

References

- EU GMP Annex 11 – June 2011
- US FDA 21 CFR Part 11 – March 1997
- MHRA 'GXP' Data Integrity Guidance and Definitions – March 2018
- Final WHO Guidance Document on Good Data and Record Management Practices – June 2016
- OECD Application of GLP Principles to Computerized Systems – April 2016
- PIC/S Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments – Aug 2016
- US FDA Data Integrity and Compliance With CGMP Guidance for Industry (Draft Guidance) – April 2016
- ISPE GAMP Records and Data Integrity Guide – March 2017
- Industry Coalition - Position Paper on Audit Trails and Audit Trail Review - Considerations Aimed at Efficiently Meeting Authorities' Requirements
- SID&GP – Guidelines - Data Integrity and Computer System Validation – Draft - 2018