Good Laboratory Practice

GUIDELINES FOR THE ACQUISITION AND PROCESSING OF ELECTRONIC RAW DATA IN A GLP ENVIRONMENT

Release Date: 29.04.2025

Version: 3.0

TABLE OF CONTENTS

1 FOREWORD

The aim of this document is to provide guidance on the GLP-compliant acquisition and processing of electronic raw data. It will aid test facilities and promote the use of a common standard, but it should not be considered as a legal document. The test facility management may use different approaches that are in compliance with the OECD Principles of Good Laboratory Practice [1, 2].

The AGIT (**A**rbeits**G**ruppe **I**nformations**T**echnologie) is a working group consisting of representatives from Swiss GLP monitoring authorities and Swiss industry with the aim of proposing procedures, which are practical for use in test facilities fulfilling GLP regulatory requirements.

The Guidelines for the Acquisition and Processing of Electronic Raw Data were originally issued in December 2005. This updated version 3.0 should be read in conjunction with the relevant OECD documents such as OECD Advisory Document No. 17, No. 17 Supplement 1 and No. 22 [3,4,5].

2 INTRODUCTION

The OECD Principles of GLP [2] describe the application of GLP Principles to studies in which raw data acquisition is mainly paper based. Nowadays, most of the instruments used in GLP studies are computerised systems and the data acquisition and processing are executed in electronic form.

In April 2016 the OECD published Advisory Document No. 17 "Application of GLP Principles to Computerised Systems" [3] addressing this situation. Furthermore, in September 2021, the OECD published Advisory Document No. 22 on GLP data integrity. This document covers all types of data but provides also specific guidance on the integrity of electronic raw data and specifies the need for documented data governance procedures to ensure data integrity. Risks to data integrity should be assessed with a data integrity risk assessment and identified risks should be reduced via adequate mitigation measures. OECD Advisory Document No. 22 also addresses the following aspects: requirement to retain dynamic data in a dynamic format, complete retention of records on all data processing activities, retention of e-mail correspondence in electronic form.

In spite of these documents, interpretation of the GLP Principles for test facilities is still considered helpful. This paper intends to provide guidance on how to apply the GLP Principles to acquisition and processing of electronic raw data considering data integrity and audit trail requirements.

3 SCOPE

This document addresses acquisition and processing of electronic raw data including data integrity aspects. Validated computerised systems are a prerequisite for these processes.

4 ELECTRONIC RAW DATA

4.1 Definition of Electronic Raw Data

Raw data are defined in the OECD Principles of GLP [2] as follows:

Raw data means all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study. Raw data also may include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognised as capable of providing secure storage of information for a time period specified by the appropriate authorities (i.e., for a time period of at least ten years as required by the Swiss Ordinance on GLP [1]).

For the purpose of the present guidelines, the definitions of the term electronic raw data and of its various forms are given below.

Electronic Raw Data:	Original records, or verified copies thereof, generated by means of computerised systems and stored on digital media. They are necessary for the evaluation and reconstruction of study results and may exist in a static or in a dynamic format as defined in OECD Advisory Document No. 22 [4].
Proprietary Form:	An electronic file format, which needs a dedicated software to be read and processed.
Human Readable Form:	A file format that can be interpreted by standard software to view the content in human readable form as text, figures, graphs, tables, etc.

4.2 Elements of Electronic Raw Data

Electronic raw data consist of the data including the associated metadata. The data represent the core data elements (measured values), whereas metadata comprise the attributes of the measured values (e.g., study number, time, sample identification) and technical properties (e.g., field properties, table relationships, etc.).

All changes to electronic raw data have to be recorded in an audit trail specifying the original and modified data, the reason for change, date and time, and the identity of the person making the change.

The processing of electronic raw data such as integration, calibration, and calculation should be described by the process itself including processing parameters, equations and statistical methods. According to OECD Advisory Document No. 22 [4] retained records should allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported.

If there are electronic and paper-based data in a study, this should be described on an index. The link between the electronic raw data and the paper data should be described to ensure data integrity.

5 DATA INTEGRITY RISK ASSESSMENT

OECD Advisory Document No. 22 highlights that test facility management (TFM) should ensure that data integrity risks are appropriately identified and controlled – for example through a data integrity risk assessment [4].
This assessment should consider all factors required to follow a process or perform an activity. It is advised to map the processes that produce, process and/or store data, identifying the data flow and the data lifecycle (see figure 1). The potential risks to data integrity should be identified, prioritised, minimised, mitigated, and, if applicable, residual risks should be accepted by TFM. The effort and resources applied to ensure data integrity should be commensurate with the risk and the impact of the associated data integrity failure.
It is recommended to perform this analysis in a multidisciplinary team (e.g., process experts, QA, study directors, IT considering also IT architecture and data security aspects [6] that may have an impact). The assessment should be revisited on a regular basis. General principles and examples of tools for quality risk management in general are provided in ICH guideline Q9 [7].

The steps in figure 1 may be considered for the data integrity risk management.

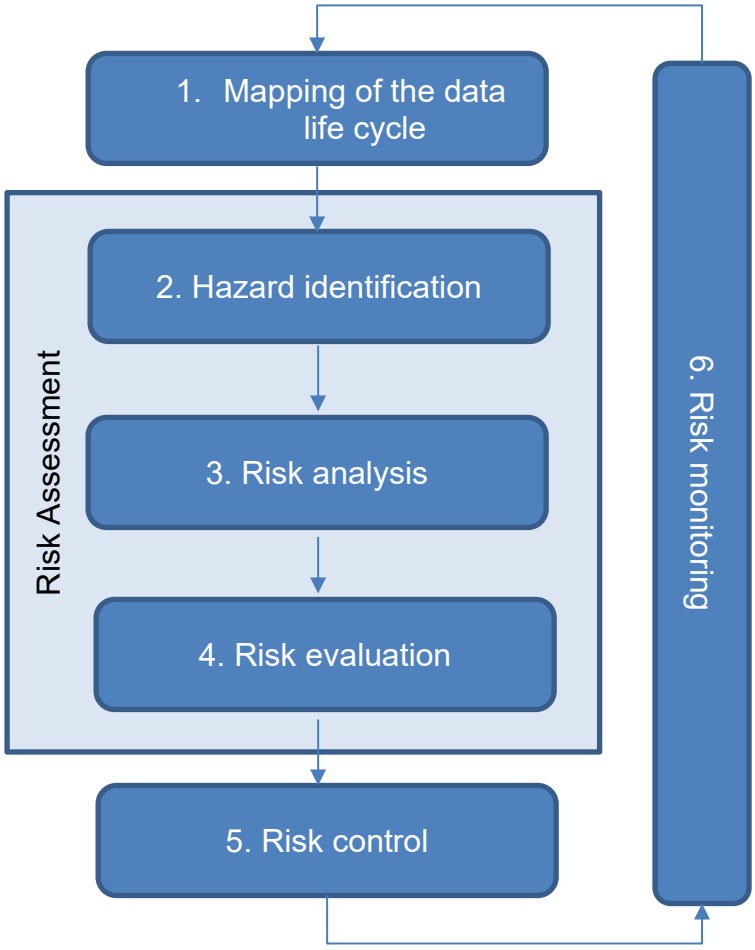

Figure 1: Risk management framework applied to data integrity (based on [7]).

5.1 Mapping of the Data Life Cycle

In a first step, the data flow throughout the data life cycle should be mapped to have a basis for the data integrity risk assessment. This description should include also the involved IT-architecture such as laboratory instruments, laboratory information management systems (LIMS), data storage infrastructure (e.g., storage and backup devices). The description should pay particular attention to data acquisition and processing and to interfaces between different systems where data transfer occurs. It may also cover other relevant aspects such as involved personnel (access privileges, potential conflicts of interest, training), locations (e.g., locations of data storage devices), data security aspects [6], etc.

The mapping should identify critical data and metadata as well as critical steps in the data life cycle. To this end, the description should also comprise a definition of which data are considered the GLP raw data including the relevant metadata. This is particularly important if data and copies thereof exist in different formats or on different media. Furthermore, also data formats and data types should be documented.

In principle, this mapping should consider each data generation process separately. However, in many cases different data generation processes will include common steps which may be assessed in a common assessment.

5.2 Hazard Identification

According to OECD Advisory Document No. 22, data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The requirements necessary to ensure data integrity are further detailed as “ALCOA+” (Data should be attributable, legible, contemporaneous, an original record (or a verified copy of it), accurate, complete, consistent, enduring, available [4].)

If one or several of these requirements are not completely fulfilled for GLP raw data, the data integrity is affected. Hazard identification means that the data flow is assessed for possible deviations from the ALCOA+ requirements which could affect data integrity (what may go wrong?).

5.3 Risk Analysis

Risk to data integrity can be defined as the product of severity of the impact of a certain hazard on data integrity and the probability of occurrence of the event.

In the risk analysis, it is also important to consider the criticality of the data affected and the detectability of impacts on data integrity [7].

5.4 Risk Evaluation

The identified risks to data integrity are to be evaluated. Based on set criteria it is decided whether and to which extent the risks are acceptable. Furthermore, the risks may be graded in order to define the extent of risk control measures necessary and to prioritise the mitigation measures.

5.5 Risk Control

Risk mitigation measures should be defined to reduce the risks to an acceptable level. These measures may include modifications of the IT infrastructure, organisational changes, supplementary documentation, or quality control measures. The residual

risks after implementation of all measures have to be identified and considered as acceptable by the TFM.

5.6 Risk Monitoring

The data integrity risk assessment is an iterative process. The mapping of the data life cycle and the data integrity risk assessment should be reviewed periodically in order to ensure that the risk assessment and the risk control are still valid. Changes in the IT-infrastructure, applications and data flow should be adequately considered, and if necessary, the data integrity risk assessment should be updated.

6 LIFE CYCLE OF ELECTRONIC RAW DATA

6.1 Introduction

The life cycle of electronic GLP raw data refers to all phases from data acquisition through processing, storage, archiving and destruction. Data integrity needs to be maintained throughout the entire data life cycle. The risks to data integrity depend on the architecture of the information technology involved as well as on the processes governing acquisition of the data and data flow along the steps in the data life cycle. The following subsections describe aspects of the IT-architecture and processes throughout the data life cycle which are critical to data integrity.

6.2 IT-Architecture

6.2.1 IT-Architecture for Data Acquisition and Data Processing

The IT-architecture refers to all aspects related to information technology in a test facility including IT-infrastructure, software, etc.

Computerised systems used for data acquisition and processing in GLP studies range from simple stand-alone laboratory instruments to instruments fully integrated into a LIMS.

LIMS are database systems designed to combine study and sample information with acquired data from laboratory instruments. The layout of the study according to the study plan can be defined in the LIMS by entering all relevant study information. Study activities such as managing the samples, data generation, data processing and documentation are performed electronically. These activities may cover all steps from preparation of data acquisition to final results of a GLP study.

Laboratory instruments such as high-performance liquid chromatography devices (HPLC), or imaging systems are equipped with instrument software. This software is designed for the acquisition, processing, evaluation, and documentation of electronic data of specific types. Processing and documentation within these laboratory instruments are generally focused on the analysis itself while LIMS are also designed for sample and study data management. However, certain data management functionalities such as assigning study attributes, e.g., study number, sample type, sampling time, and providing access control and audit trail are also part of the software of laboratory instruments.

The level of laboratory instrument integration into a LIMS depends on the complexity of the instrument itself and the functionality of the LIMS. Any level of integration from stand-alone laboratory devices to fully integrated systems is possible; figure 2 visualises the following examples:

1. In absence of a LIMS, the sequence preparation and data acquisition occur on stand-alone laboratory instruments. Data processing and data reporting may occur on separate systems (see figure 2, case 1) or directly on the laboratory instrument.
2. The operation of the instrument and the preparation of the sequence and the data acquisition are controlled by instrument software. Data entry into the LIMS is performed by the operator. Transfer to the LIMS should be performed in a timely manner ensuring data integrity and traceability. Data processing and data reporting may occur on separate systems (see figure 2, case 2) or directly on the laboratory instrument.
3. The operation of the instrument and the data acquisition are controlled by instrument software. The LIMS manages sequence preparation, data entry and is used for data reporting. Data processing can occur on a separate system (see figure 2, case 3) or on the same system as data acquisition.
4. A fully integrated LIMS controls the operation of the instrument including sequence preparation, data entry, data acquisition, data processing and data reporting (see figure 2, case 4).

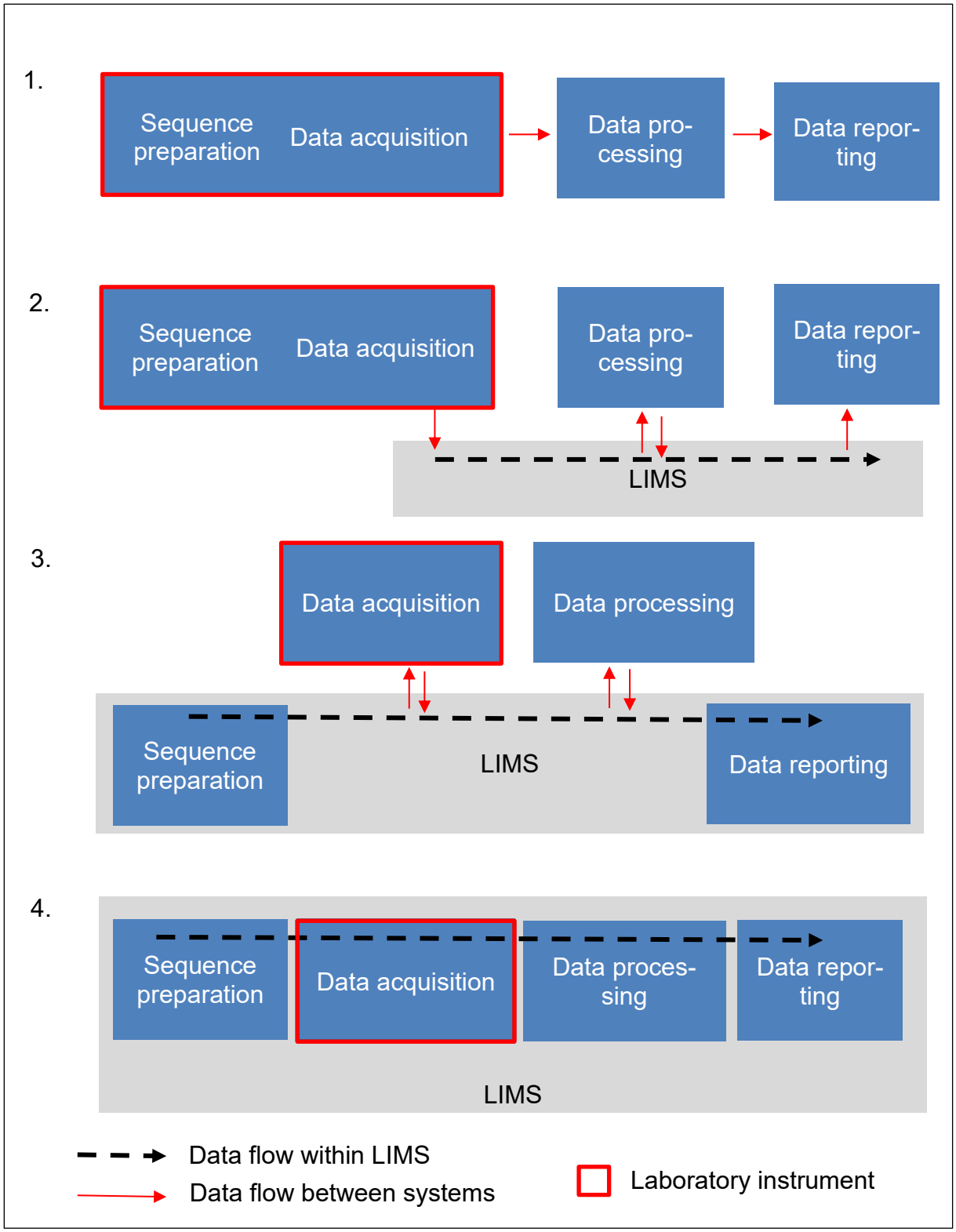

Figure 2: Degree of instrument integration in the Laboratory Information Management System (LIMS). From stand-alone laboratory instruments (1.) to fully integrated systems controlled by the LIMS system (4.).

6.2.2 Data Storage and Backup Infrastructure

After acquisition and processing, the GLP raw data should be safely stored, and backup procedures need to be in place (see section 6.8). The corresponding IT-architecture and data flows should also be subject to the data integrity risk assessment. In case the data flows are controlled by automated processes, the aspect of data integrity should be covered by computerised system validation. In case of manual transfer of data, additional measures may be necessary to demonstrate that data integrity is maintained. For archiving of electronic raw data see AGIT Guidelines for the Archiving of Electronic Raw Data in a GLP Environment [8].

6.2.3 Impact of IT Architecture on Data Integrity Risks

The data integrity risk assessment should pay particular attention to the level of integration. If a LIMS is available, its functions and its interaction with the laboratory instruments and the corresponding interfaces should be clearly described.

If stand-alone laboratory instruments are used for the acquisition and processing of electronic raw data, the requirements regarding access control, data transfer, backup, disaster and recovery control may be challenging and need dedicated solutions to ensure data integrity. These aspects should be evaluated in the data integrity risk assessment.

For fully integrated instruments managed by a LIMS, the risk assessment regarding data integrity is the basis for the validation of the instrument (see AGIT Guidelines for the Validation of Computerised Systems [9]).

It is necessary to decide on a case-by-case basis, whether a software solution meets the requirements for data integrity. The data integrity risk assessment may identify areas for remediation. In case limitations are identified, they should be mitigated (e.g., by supplementary offline documentation, specific technical solutions, organisational processes).

Examples of factors that may pose a risk to data integrity, some of these factors are discussed in more depth in the next sections – main impact to ALCOA+ is in brackets:

- Missing data or metadata (data may not be complete, consistent, or attributable)
- Incomplete audit trail function of instrument software (see chapter 7) (data may not be complete or attributable)
- Incomplete data transfers (including transfer of metadata) from one system to the other (data may not be complete/consistent)
- Use of generic login accounts (data is not attributable)
- Incomplete recording and retention of data processing activities (data may not be complete or enduring)
- System time/date settings not being protected against modifications (it may be difficult to ensure data is contemporaneous if timestamp is impacted)
- Static format used for retention of dynamic raw data (data may not be complete)
- Limited possibilities for backup of data on stand-alone laboratory instruments, manual backup procedures (it may be challenging to ensure data is enduring)

- Changes in software or software version, without proper impact assessment on existing data (may impede legibility of data)
- Cyber-attacks may lead to loss of information or unauthorised access or changes (affects completeness, availability of data)

6.3 Data Acquisition

6.3.1 General Requirements

The requirements for raw data acquisition are described in the OECD Principles of GLP [2] as follows:

All data generated during the conduct of the study should be recorded directly, promptly, accurately, and legibly by the individual entering the data. These entries should be signed or initialled and dated.

Any change in the raw data should be made so as not to obscure the previous entry, should indicate the reason for change and should be dated and signed or initialled by the individual making the change.

Data generated as a direct computer input should be identified at the time of data input by the individual(s) responsible for direct data entries. Computerised systems should always provide retention of full audit trails to show all changes to the data without obscuring the original data.

6.3.2 Planning and Preparation of Data Acquisition

The experimental procedures in the study plan are carried out in the laboratory and translated to instrument configurations. Measurement sequences are defined in the LIMS system or in the instrument software. Analytical methods and, if applicable, also data processing procedures are implemented.

During these activities, the physical samples placed into the instrument, or the series of samples placed on the autosampler should be unambiguously linked with the sample descriptor in the LIMS or in the measurement procedure or measurement sequence in the instrument software.

Errors in instrument calibration, analytical method definition, attribution of sample descriptors in the measurement sequence may affect the accuracy of data (data do not represent what was intended to be measured).

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
Measurement sequence on the instrument is edited manually. Samples descriptors are attributed according to the sample list and samples are loaded on the autosampler of the instrument. If they are mixed up, they will not correspond to the programmed sequence.	Accurate	Organisational measures, e.g., second person review, to verify the correct sequence.

6.3.3 Manual Data Acquisition or Data Handling Steps

In many cases, data acquisition processes are not fully automated and manual interaction is required. Data entry into the system may occur directly via keyboard, data

acquisition processes can be initiated manually on stand-alone laboratory instruments (single or batch acquisition process). There may be possibilities for manual modification of data after acquisition. Furthermore, data may have to be transferred manually to a storage medium or to the LIMS after acquisition. These manual data handling activities require particular attention in the data integrity risk assessment.

Manual data entry: If data are to be entered directly into a computerised system, the necessary metadata on user identification, time of data entry etc. are required. Failure to record these metadata (e.g., if flat files are used or if a software does not support corresponding audit trail functions) constitutes a deviation from GLP, data integrity requirements are not met.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
The software used for manual data entry records the user identification and the time of data entry. However, only a generic account is used by lab personnel.	Attributable	Personalise the account if technically possible or maintain a logbook to identify the user who performed the actions.

Manual correction of data: If data need to be corrected, the original record, the modified record and the reason for change as well as the person who modified the record and a time stamp are to be documented. This requires suitable audit trail functions (see chapter 7). In any case, changes to electronic raw data should be detectable.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
The data generated from the laboratory instrument can be modified but the reason for change is not recorded in the audit trail.	Complete	Activate the complete audit trail functionality or maintain a logbook to record the reason for change and link it adequately to the electronic data.

Manual initiation of data acquisition: A data acquisition process is initiated manually on a stand-alone laboratory instrument, which is not controlled by a LIMS. The measurement parameters and/or measurement sequences are entered directly on the system and the data acquisition is initiated manually.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
The system date and time is not updated automatically e.g., for summertime or after power outage.	Contemporaneous	Generate a procedure to ensure that all systems are set to the correct date and time.

6.3.4 Fully Automated Data Acquisition and Transfer of Data into the LIMS

Fully automated data acquisition and transfer into the LIMS is possible when, the laboratory instruments are fully integrated into the LIMS. Data acquisition is initiated via the LIMS based on the study design. The LIMS communicates directly via an interface with the laboratory instrument. The measurement sequence on the instrument runs in a continuous batch acquisition process (e.g., HPLC runs using an autosampler, blood analyses performed by a bioanalysis system). The electronic raw data generated by the analysis will be automatically entered into the LIMS during the acquisition process. The individual responsible for electronic raw data acquisition is the person who starts the process of data acquisition in the LIMS.

This is also valid for data acquisition processes running over a longer period of time, e.g., temperature and humidity in an animal room or in environmentally controlled areas. In case of fully automated data acquisition, data integrity is an aspect which needs to be covered by the computerised system validation. The requirements regarding data integrity (including for example audit trail requirements, completeness of data transfers, readability of generated data) need to be reflected in the user requirement specification. The risk assessment regarding data integrity is an integral part of the risk assessment which is conducted as basis for the computerised system validation. The validation of the computerised system needs to demonstrate that data integrity is maintained throughout the entire data acquisition process (see AGIT Guidelines for the Validation of Computerised Systems [9]).

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
Data acquisition on the laboratory instrument occurs based on the measurement sequence generated in the LIMS. The laboratory sequence from the LIMS may not be correctly interpreted by the laboratory instrument which may lead to incorrect method parameters and incorrect measurement sequence. After a change in the software of the instrument, the measurement sequence is no longer correctly interpreted.	Accurate	The computerised system validation needs to demonstrate that measurement sequences generated in the LIMS are correctly interpreted and executed by the laboratory instrument. Change management should ensure adequate impact analysis of planned changes and the validation process should be initiated.

6.4 Data processing

Some acquired electronic raw data already represent final results, e.g., weight, temperature, humidity. Other acquired electronic raw data, such as intensity values correlated with time or wavelength and generated by chromatography, spectroscopy, etc. need further processing to obtain final results (e.g., retention times, peak areas, and concentrations).

These processes, such as integration of chromatographic peaks and calibration, are defined by processing parameters or calibration factors. They do not affect the initially acquired data but the resultant data after processing. The processing parameters may be changed during data evaluation. The changed processing parameters, methods, and processed data should be clearly identified.

According to OECD Advisory Document No. 22 [4], all records should be retained, regardless of whether the output of that processing is subsequently reported. Based on the study documentation it needs to be traceable which data (initially acquired data or processed data) were used for the study report. In case data were not reflected in the final report, for example if data acquisition or processing had to be repeated, a justification should be available.

Example of data processing: The default integration parameters (slope, minimum peak area) of a HPLC method result in an inappropriate integration of the run due to a large number of noise peaks (see figure 3 first evaluation). The integration parameters were optimised until an acceptable evaluation was obtained resulting in the integration of the relevant peaks only (see figure 3 second evaluation). After structural elucidation and co-chromatography with reference items an assignment of the corresponding metabolite fractions was possible (see figure 3 third evaluation). All intermediate results obtained during the first and second evaluations should be retained, even if they are not reflected in the final report. The selection of the processed data for the final report should be justified.

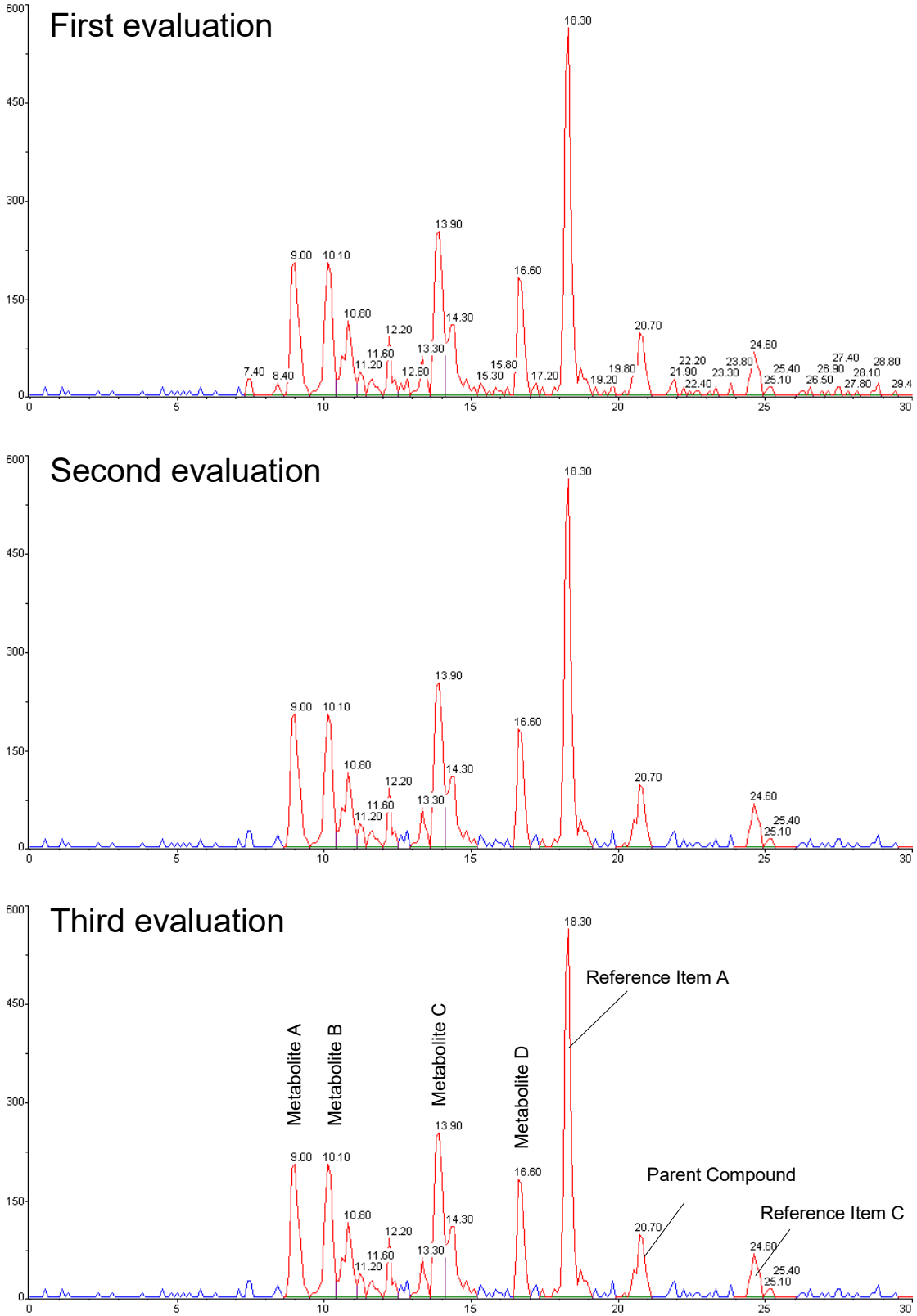

Figure 3: Examples of processing HPLC data. Data obtained with the processing parameters of the HPLC method (first evaluation), integration of the relevant peaks only by selecting optimised integration parameters (second evaluation) and peak assignment based on structural elucidation and co-chromatography with reference items.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
Data processing parameters can be modified and a metabolite at low concentration may be lost. These data processing activities are not completely recorded.	Attributable, contemporaneous, accurate	Requirement for documentation of all data processing activities and retention of all processed data.

6.5 Data Review

Critical data are subject to a data review for quality control (see OECD Advisory Document No. 22). Data review for quality control may be conducted by the study director or other personnel. The data should be reviewed according to a procedure which defines the actions to be taken in case of deviations. The data review should pay attention to data integrity aspects and may include a review of the audit trail (see chapter 7). The data review and any action taken as a consequence of deviations should be documented.

6.6 Data Migration

Data migration procedures may involve transfers from one IT-system to another or from one data format to another. Data transfer processes need to be designed in a way that the integrity of the transferred data is maintained.

For example, if electronic raw data are transferred from the proprietary form to a human readable form, the relationship between measured values and their metadata has to be maintained. If data generated in a dynamic format is transferred, the dynamic status of the data with all relevant attributes needs to be maintained. The transfer processes need to ensure that all data including all metadata are transferred.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
Data acquisition occurs on an infrared spectrometer. The instrument is not integrated in the LIMS in which the study data is managed. The generated electronic raw data files of the analysis will be stored locally on the instrument computer. A subsequent manual transfer of the different data files to the LIMS is necessary. The manual transfer of the data may not be complete; some files could be missed.	Complete	A documented check of completeness of the transferred files is conducted based on the documentation of the recorded spectra.

6.7 Data Storage

The GLP Principles require that all necessary information to reconstruct a study are retained. This includes the GLP raw data including associated metadata and processed data. The systems used need to be validated and the processes involved should be subject to the data integrity risk assessment. Risk to data integrity is posed

for example by data loss due to corruption of storage media, unauthorised access and modification/deletion of data, impaired readability due to software updates.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
The servers used for data storage may be affected by a flooding event.	Complete, enduring, available	Installation of water sensors, backup to a server located in another building of the facility.

6.8 Backup Procedures

When data are stored and archived electronically, adequate backup and data recovery procedures need to be in place [3,4,6]. In case the stored data are damaged by an incident, it may be necessary to replace the stored data by the data on the backup device. Therefore, the data integrity risk assessment should also cover the backup and data recovery procedures.

Example for risk to data integrity:

Risk identification	Affected ALCOA+ criteria	Mitigation measures
In a HPLC-system, the raw data generated are stored on the instrument computer after acquisition and then transferred to another storge medium after the sequence has been completed. Backups of the data on the instrument computer are taken on a weekly basis. If a corruption of the storage system occurs just before the backup is taken, the data generated during this week will be lost.	Complete, enduring, available	Adapt the backup frequency to the frequency of data changes on the system.

6.9 Archiving

Electronic raw data should be archived after completion of the study (when the final report is signed by the study director) as for all other study raw data (paper, specimens etc.). The data integrity risk assessment should also cover retention of electronic raw data, transfer to and storage in the archive. Detailed requirements for archiving of electronic raw data are described in the separate AGIT guidelines [8].

7 AUDIT TRAIL

This AGIT guidance document focuses on the data audit trails, which are records of all events that occur to data. The data audit trail may be a part of the system audit trail, which records all events that occur to a system.

7.1 Audit Trail Requirements

The requirements for an audit trail are described in the OECD Principles of GLP [2] as follows:

Computerised system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original data. It should be possible to associate all changes to data with the persons having made those changes, for example, by use of timed and dated (electronic) signatures. Reason for changes should be given.

An audit trail allows reconstruction of the course of changes to electronic raw data and provides evidence of data integrity. The audit trail should be generated by the computerised system and contain information about what, when, who, and why.

The audit trail should be an additional unalterable electronic record, which should always be switched on during GLP activities.

According to OECD Advisory Document No. 22 [4], *the ability to make modifications to the audit trail settings should be restricted to authorised personnel. Any personnel involved in a study (e.g., study directors, heads of analytical departments, analysts, etc.) should not be authorised to change audit trail settings.*

Regardless of the technical solution, the audit trail should be inseparably linked to the corresponding electronic raw data in a logical or physical way and have the same retention requirements as the data. The system should be able to highlight alterations of the original raw data, the initial entry and the change applied should be visible.

Timestamps in the audit trail should indicate year, month, day, and the time providing an adequate level of precision (e.g., time zone). Procedures should be established to control the integrity and accuracy of the computer time used for the timestamp. Particularly, access to the computer time should be protected against unauthorised changes.

The audit trail does not require an electronic signature, attributability to the person performing the action via a user authentication procedure is sufficient (see section 8.2), but in case of changes to the electronic raw data, a justification is mandatory.

The audit trail should be available in a human readable form. Search, query and sort functions are desirable.

An audit trail differs from a log file. A log file records all activities (such as login, data entry, changes, and approvals) of a computerised system in a sequential, chronological order. The availability of a log file facilitates the traceability of all activities on the computerised system, but it is not a GLP requirement.

7.2 Audit Trails in Different Systems

The need for an audit trail depends on the level of system complexity, system functions and risk to data integrity.

Audit trail functionalities may differ depending on equipment and the incorporated software.

7.2.1 Computerised Systems Which Do Not Allow Data Changes

When a computerised system does not allow any data modification, such as a data logger used to record temperature with adequate data storage, an audit trail is not required.

7.2.2 Computerised Systems Allowing Data Changes

Computerised systems such as analytical systems are usually provided with an audit trail function to record the required information and allow an audit trail review. The

understanding of “audit trail” by suppliers may vary and the audit trail functions may not always comply with GLP-requirements. In case the audit trail functionalities do not comply to the GLP-requirements to full extent, these shortcomings should be mitigated with other measures to ensure quality and integrity of the data (see [4]). The approach chosen should be documented in an SOP, which describes the information to be collected and how this information has to be documented and retained.

7.3 Audit Trail Review

As emphasised in the OECD Advisory Document No. 22, a data audit trail is part of the data integrity requirements through the data life cycle.

A review of the audit trail should be performed by the study director [4] and during inspections of the study report and raw data by QA [10]. The extent (depth and frequency) of the audit trail review should be determined based on a risk assessment. The review may be limited to activities with GLP relevance (e.g., relating to data creation, processing, compliance with procedures, modification and deletion, etc.).

The audit trail review process and reporting should be described in an SOP including roles and responsibilities and should be part of the quality assurance programme

Examples of potential issues identified by audit trail review are:

- Incomplete correction of erroneous data entry
- Changes by unauthorised persons
- Data not entered contemporaneously
- Falsification of data entry

8 ELECTRONIC SIGNATURE VERSUS IDENTIFICATION

8.1 GLP Requirements for Electronic Signatures

A signature is legally binding and expresses a certain act in relation to the document signed (e.g., review, approval, endorsement). In the following cases a dated signature is mandatory according to the OECD Principles of GLP [2]:

- Approval of the study plan, final reports and their corresponding amendments by the study director
- Approval of the study plan by the test facility management [1]
- Reports of principal investigators or scientists involved in the study
- Quality assurance statement

In cases where study plan(s) and report(s) are generated and maintained in an electronic form, electronic signatures are applicable. The specific requirements for electronic signatures are outlined in OECD Documents No. 17 and 22 [3,4].

8.2 User Identification

Initialling of electronic raw data by the user is ensured by a unique identification of an individual obtained at application log on (for more details see OECD Document No. 25 [6]).

The entry and acquisition of electronic raw data should be inseparably linked to the user identification and time stamp.

Unauthorised use of open sessions should be prohibited. Short timeout intervals appropriate to the working process should be implemented, e.g., 10 minutes. In addition,

accounts should be locked after a pre-defined number of successive failed authentication attempts [6].

The identification of users and the time stamp of each data entry should be easily retrievable from the system.

9 ROLES AND RESPONSIBILITIES

Only authorised users should have access to the computerised systems. For each individual system a clear assignment of users, roles and privileges should be defined and documented.
Regarding potential conflicts of interest with regard to user or system administrator access, see OECD Advisory Document No. 22, section 8.2 [4].

9.1 Test Facility Management

The management of the test facility has overall responsibility for compliance with the GLP Principles. In particular, the management has to establish procedures to ensure that computerised systems are suitable for their intended purpose, and are validated, operated, and maintained in accordance with the Principles of GLP. TFM should ensure that all personnel involved in acquiring and processing electronic raw data are well trained in using the relevant applications.

9.2 Study Director /Principal Investigator (PI)

The study director is responsible for the overall conduct of the study and the GLP compliant acquisition and processing of electronic raw data for that study. The study director should have access rights to all electronic raw data pertaining to the study and the corresponding audit trails. The study director is responsible for approvals of the electronic raw data and calculated results. If necessary, the right to approve data may be delegated by the study director to a principal investigator, senior member of staff, or another specifically trained person. This delegation should be documented. However, the responsibility always remains with the study director.

If the study director or PI enters or modifies data, the corresponding points in section 9.3 apply.

9.3 Study Personnel

The technical personnel are responsible for the quality of their data. The acquisition of electronic raw data should be performed in compliance with the GLP Principles, i.e., prompt and accurate recording of the electronic raw data. Once electronic raw data have been entered into the system, it is not permitted that they are obscured or deleted. For all changes to these data a meaningful reason for change should be given and recorded in the audit trail. The study personnel are responsible for secure handling of user IDs and passwords. Unauthorised access should be prevented, e.g., by logging out.

9.4 Quality Assurance (QA)

The quality assurance personnel should have read-only access to all systems containing electronic raw data. The QA personnel should be trained in using the systems, so that they can review all electronic raw data and audit trails during report audit and inspections.

9.5 System Administrator

The system administrator is responsible for user registration and for assigning defined access rights. All changes should be documented in order to have an overview of all registered users, their functions, access rights, and period of access. In particular, it is necessary to document the user authorisation history (users entering and leaving the test facility or changing their responsibilities).

10 REFERENCES

[1] Ordinance on Good Laboratory Practice of 18 May 2005 (Status as of 1 December 2012) [RS 813.112.1]. (OGLP)

[2] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 1: *OECD Principles on Good Laboratory Practice (as revised in 1997)*, OECD Publishing, Paris, 1998. (OECD)

[3] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 17: *Advisory Document of the Working Group on Good Laboratory Practice, Application of GLP Principles to Computerised Systems*, OECD Publishing, Paris, 2016. (OECD)

[4] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 22: *Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity,* OECD Publishing, Paris, 2021. (OECD)

[5] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 17 Supplement 1: *Advisory Document on GLP & Cloud Computing*, OECD Publishing, Paris, 2023. (OECD)

[6] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 25: *Position Paper on Good Laboratory Practice and IT Security*, OECD Publishing, Paris, 2024. (OECD)

[7] International Council on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH): ICH Harmonised Guideline, Quality Risk Management, Q9 (R1) 18 January 2023. (ICH)

[8] Working Group on Information Technology (AGIT): *Guidelines for the Archiving of Electronic Raw Data in a GLP Environment*. (AGIT)

[9] Working Group on Information Technology (AGIT), *Guidelines for the Validation of Computerised Systems.* (AGIT)

[10] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 23: *Advisory Document of the Working Party on Good Laboratory Practice on Quality Assurance.* OECD Publishing, Paris, 2022. (OECD)

11 WORKING GROUP ON INFORMATION TECHNOLOGY

The Working Group on Information Technology (AGIT) was founded on 27 March 1998 with the objective of discussing relevant topics of Good Laboratory Practice (GLP) in the field of information technology between industry and the monitoring authorities. The list of the current members of the AGIT (i.e., invited experts from industry and representatives from the Swiss GLP monitoring authorities) is available in the AGIT section on the Swiss Good Laboratory Practice (GLP) website.

The AGIT provides guidelines based on legislative requirements and practical experience to support test facilities in applying the GLP Principles to information technology. AGIT publications are available on the Swiss Good Laboratory Practice (GLP) website (AGIT section).