Good Laboratory Practice

GUIDELINES FOR THE VALIDATION OF COMPUTERISED SYSTEMS

Release Date: 29.04.2025

Version: 4.0

TABLE OF CONTENTS

1 FOREWORD

The aim of this document is to provide guidance on the GLP-compliant validation of computerised systems. The guidance should aid test facilities and promote the use of a common standard but should not be considered as legally binding. A test facility management may use different approaches, as long as they are in compliance with the OECD Principles of Good Laboratory Practice [1,2]. The extent of a validation may vary depending on the criticality and complexity of the computerised system. In any case the validation should demonstrate that the computerised system is suitable for its intended purpose.

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 Validation of Computerised Systems were originally issued in June 2000. This updated version 4.0 should be read in conjunction with the relevant OECD documents such as OECD Advisory Documents No. 17, No. 17 Supplement 1 and No. 22 [3,4,5].

2 INTRODUCTION

The validation of computerised systems is required by the OECD Principles of Good Laboratory Practice [2]. OECD Document No. 17 provides a detailed description of the application of the Principles of GLP to computerised systems and specifies what is needed for the life cycle of computerised systems in a GLP regulated environment. It puts an emphasis on risk assessment as the central element of a scalable, economic and effective validation process with a focus on data integrity [3].

The OECD GLP Principles and OECD Document No. 17 define validation as "*action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring and demonstrating the fitness for its purpose".* The validation process provides a high degree of assurance that a computerised system meets its pre-determined specifications.

3 SCOPE

The present guidelines are an interpretation of the OECD GLP Principles regarding computerised systems and the corresponding OECD documents and gives guidance for practical implementation of these principles to the validation of computerised systems that are used in a GLP environment. These guidelines recommend conducting computerised system validations in analogy to GLP studies, however other approaches are also acceptable.

4 COMPUTERISED SYSTEMS

4.1 Definition

In OECD Document No. 17 a computerised system is defined as follows: "*A computerized system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating*

procedures performed by personnel" [3]. The system might include virtual components hosted locally or in a cloud [4]. A generally accepted model of a computerised system is depicted in Figure 1.

Computerised systems can vary in complexity from simple stand-alone systems to a laboratory instrument integrated into a Laboratory Information Management System (LIMS) with multiple functions. The aim of the validation remains the same for all systems, namely, to demonstrate the suitability of the system for its intended purpose. However, depending on the criticality and complexity of a system the extent of testing and documentation may differ significantly.

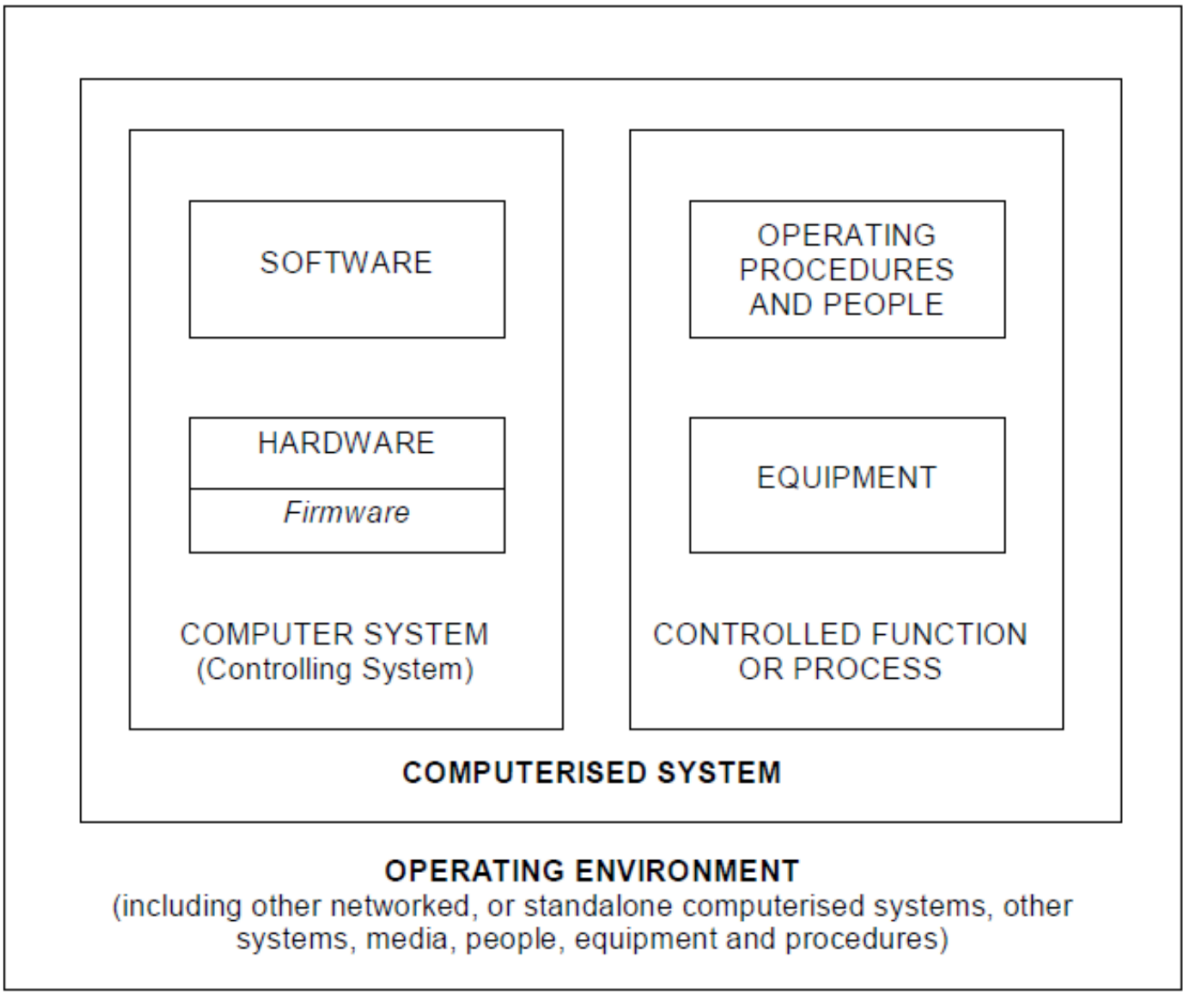

Figure 1: Definition of a Computerised System, hardware consists of the physical components of the computerised system; it includes the computer unit itself and its peripheral components. Software is the program or programs that control the operation of the computerised system [3, 6].

The model in Figure 1 describes a vast range of possible systems. The computer system in a LIMS will be more complex (server, network, database, clients, etc.) than for a laboratory instrument connected to a standalone PC. Cloud-based systems can include hardware, operating systems, application software, depending on the service model [4].

4.2 Which Systems Should Be Validated?

"All computerised systems used for the generation, measurement, calculation, assessment, transfer, processing, storage or archiving of data intended for regulatory

submission or to support regulatory decisions should be validated, and operated and maintained in ways that are compliant with the GLP Principles. The same requirement also applies to computerised systems used to produce other GLP-relevant data such as records of raw data, environmental conditions, personnel and training records, maintenance documentation, etc." [3].

As a first step, it should be clarified if the system is GLP-relevant.

The following questions may guide the decision on the GLP relevance of the system:

- Will the system be used to produce, process, or maintain data that are intended to be used in regulatory submissions?
- Will the system be involved in the environmental control processes (e.g., temperature, humidity, light) of test systems, test items or specimens used in GLP studies?
- Is the system part of a process liable to inspections by GLP monitoring authorities (e.g., electronic document management system for SOPs or training records)?

If the answer to any of these questions is yes, the system is GLP relevant and it needs to be evaluated, whether the system requires validation. According to OECD Document No. 17 [3], for lower complexity systems a formal qualification may be acceptable. Since this decision should be taken for each individual computerised system, it may be helpful to define categories of systems with the corresponding assignment to a validation process or function control tests in an SOP. For example:

Category A: Exempted Systems not requiring validation, calibration or function control tests

Category B: Simple computerised systems requiring calibration and function control tests to demonstrate the system is fit for purpose

Category C: Complex computerised systems requiring validation

Criteria to be considered when categorising the systems include the following:

- Complexity of the system and the software
- Degree of configuration or customisation of the system or the software (i.e., non-configurable commercial of the shelf system vs. custom-developed system)
- Whether the system's functions include data storage or data transfer procedures (e.g., transfer to a LIMS)

A centrifuge, which does not require calibration may be considered as an exempted system (category A). A stand-alone balance not generating electronic data may be assigned to category B. A chromatography system or any instrument which is part of a LIMS always requires validation (category C).

5 VALIDATION PROCESS

5.1 Validation Framework

The test facility management establishes the general framework for validation of computerised systems in compliance with the OECD GLP Principles. This framework

should cover and define all general validation aspects for the entire life cycle of computerised systems.

This framework may include documents such as the validation master plan, system inventory, general SOPs on validation including risk assessment aspects.

5.2 Defining the Scope of the Validation

The scope of the validation should be clearly defined, highlighting all components the system is comprised of. Because the validation of a laboratory instrument as an integral part of a LIMS is complex, it may be more practical to validate the equipment separately from the LIMS to which it is connected. In this case, the interface between the laboratory instrument and the LIMS should be tested as part of the validation of either the LIMS or of the laboratory instrument.

5.3 Risk Assessment

A documented risk assessment is necessary to determine the validation approach and to scale the validation effort accordingly [3]. The validation effort should align with the complexity and intended use of the system as well as the risks to data quality and data integrity. This risk assessment ensures the efficient allocation of resources to critical aspects and functions of the system.

Conducting the risk assessment requires a detailed description of the system, including its interfaces, functions, IT security aspects, involvement in the data life cycle stages, as well as user requirements and specifications. Furthermore, the supplier`s services and quality standards should be taken into account. Conducting a supplier audit can be considered (see section 5.6).

The risk assessment should encompass, though is not restricted to, the following aspects:

System
In assessing risks, particular attention should be given to the properties and setup of the system. Typically, risks increase with greater system complexity and customisation. It is essential to scrutinise the system for elements such as non-standard interfaces, customised configurations and custom-coded software components, all of which pose increased risks and necessitate a more thorough validation effort.

Functions
The risk assessment based on user requirements and system specifications should establish the impact of the system functions on GLP compliance and their probability of failure. The extent of validation will have to be scaled based on the probability and impact of failure of the function. Computerised systems may have an extensive number of functions; however, only the functions required for GLP purposes need to be validated in a GLP compliant manner.

Data integrity
There is a requirement to identify and control risks throughout the entire data life cycle for GLP data [5]. For computerised systems, assessing the risk to data integrity is essential for determining the validation approach and its extent. The risk assessment should consider the criticality of data and identify processes, functions, system components, and interfaces that present risks to data integrity, necessitating special attention during validation.

The outcome of the risk assessment will guide the validation team regarding the extent of validation. Validation activities, such as testing, and maintenance as well as the corresponding SOPs should consider the preservation of data integrity throughout the life cycle of the data and the system.

Risk assessment considerations should also be taken into account when changes are made to the system to scale change control activities [3,7].

5.4 Conduct of a Validation

The GLP Principles allow some flexibility in carrying out validations. This guideline proposes performing validations analogue to GLP studies as this has a number of advantages:

- This approach facilitates compliance with the Principles of GLP and the general understanding of the procedures by the parties involved.
- The GLP Principles specify in detail the content of the study plan, the conduct of a study, reporting of study results, storage and retention of records.
- They require the assignment of responsibilities and the availability of SOPs.

All these considerations can conveniently be applied to computerised system validation as shown in the table below.

Table 1: Computerised System Validation (CSV) analogies to a GLP Study

GLP Study	**CSV**
Study Director (SD)	Validation Director (VD)
Study plan	Validation plan
Method description	Test scripts
Conduct of study	Conduct of testing
Study raw data	Validation raw data
Study report	Validation report

A generic validation performed by the supplier is usually not sufficient as validations should be specific to the processes conducted at the test facility. However, where appropriate, test plans, test scripts or other documents provided by the supplier may be used or adapted to the specific situation. If the test facility relies on validation activities conducted by the supplier, these activities and the corresponding documentation need to be evaluated by the test facility.

5.5 System Development Life Cycle

The V-model in Figure 2 gives an overview of the different phases during a system development life cycle.

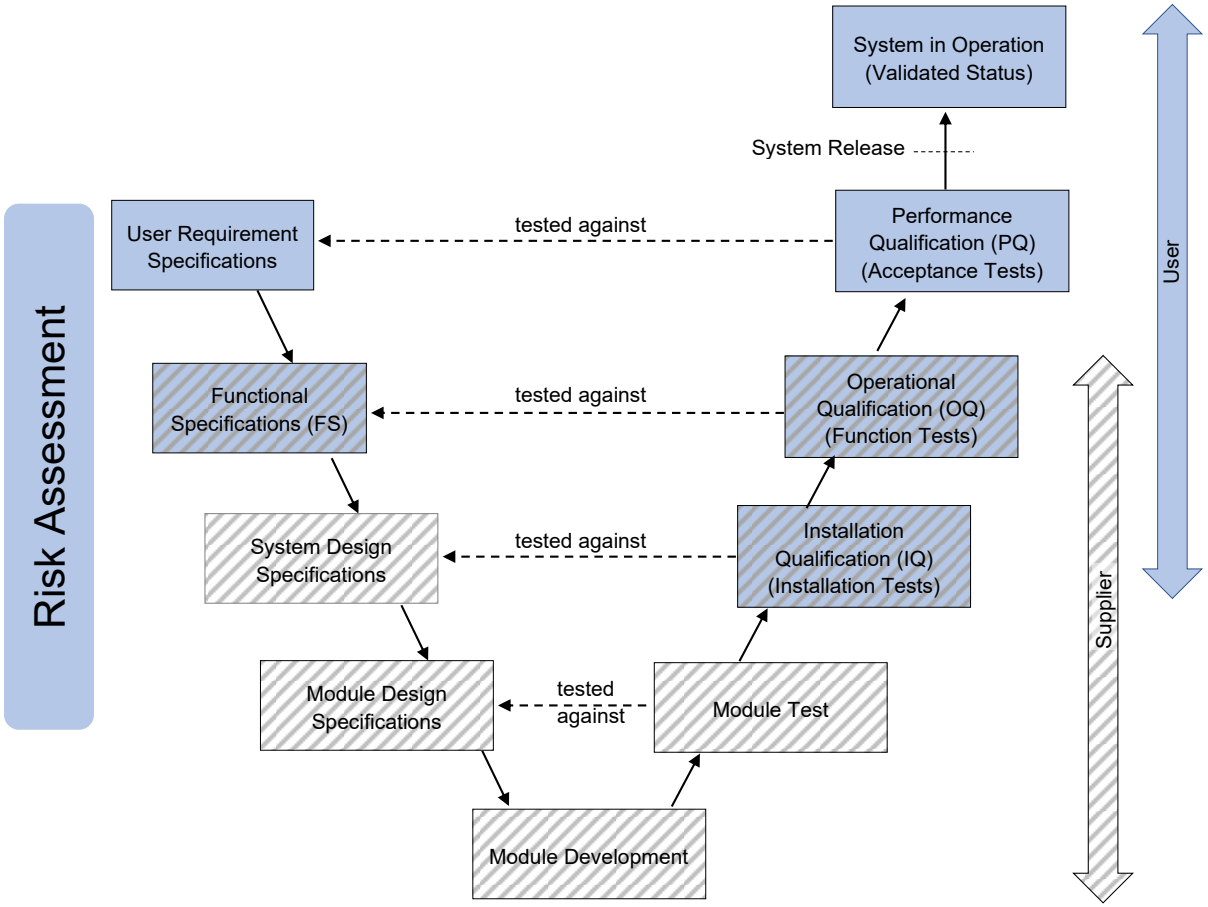

Figure 2: The V-model describes the system life cycle. The processes in the shaded boxes can be performed by the supplier or by the supplier in cooperation with the user.

Different methodologies (e.g., agile development) may also be used - in this case, the validation plan (or any other relevant document, for example a dedicated system development lifecycle SOP) should explain the different activities, verifications and documents needed to demonstrate that the user requirements are fulfilled.

User Requirement Specifications (URS)
The users formally compile all requirements in a document called user requirement specifications**.** These URS contain scientific, business, regulatory, security, data integrity (including audit trail requirements), performance and quality aspects of the future system and should cover all GLP-relevant functions of the system. During the process of defining the URS it is necessary to differentiate between essential and desirable requirements. The essential requirements for the intended purpose should be unequivocal and testable. The user requirements serve as the basis for the User Acceptance Testing, also referred to as Performance Qualification (PQ).

Functional Specifications (FS)
In case of a custom-built system, the supplier (in cooperation with the user, if applicable) translates the URS into FS. However, if the user prefers to purchase a commercially available product, the FS have been predefined by the supplier. Therefore, the user should determine if the offered functionalities of the product meet the URS.

System Design/Configuration Specifications
These specifications describe the design and configuration of all the necessary system components such as hardware, equipment, software, operating system and network components. All components that are specifically developed for a computerised system should be further defined in module design specifications.

Module Design Specifications/Development/Testing
The definition of the module design specifications as well as the development and testing of the individual modules are performed by the developer and/or supplier. Thus, the user is not directly involved but should ensure that the system was developed according to commonly accepted standards, e.g. by a (supplier) audit.

Installation Qualification (IQ)
IQ or system installation testing builds upon the system design specifications. It shows that the system has been properly installed in the user's environment and that all components are operative. This qualification can be performed by the supplier in cooperation with the user.

Operational Qualification (OQ)
The OQ should demonstrate that all functions needed for the intended purpose are available and operate reliably in the user's environment. It can be performed by the supplier and/or user.

In case of a supplier purchased system, available OQ test scripts, which will be executed by the supplier at the user's site should be reviewed by the user. Based on this review, additional test scripts might be developed and executed by the user and/or supplier to ensure sufficient testing of all important functions.

Performance Qualification (PQ)
The PQ should demonstrate that a computerised system is suitable for its intended purpose in the user's own environment. The URS should be tested in the PQ phase.

System in Operation
After successful completion of all qualification phases, including documentation (see Chapter 9), the validation is completed by the validation director signing and dating the validation report. The system should be released for operational use by the test facility management. The test facility management can delegate system release to the system owner. The test facility management should ensure that all personnel operating the system are trained and that the necessary SOPs about using and maintaining the system are in place.

Change Control
Changes during the validation should be controlled and documented in the validation documentation and tested, if necessary. For more details see OECD Advisory Document No. 17 [3].

Regarding change control during the operational phase see also AGIT Guidelines for *Change Management and Risk Assessment of Validated Computerised Systems in a GLP Environment* [7].

5.6 Supplier Audit

If suppliers, including internal service providers, are involved (e.g., in developing, operating the system or in providing validation services), written agreements should be available, and a supplier audit may be necessary (see OECD Document No. 17 [3]).

6 RESPONSIBILITIES AND DOCUMENTS

The responsibilities for a validation are extensively described in OECD GLP Document No. 17. The main responsibilities can be summarised as follows:

The **test facility management** (TFM) has overall responsibility for compliance with the GLP Principles. In particular TFM should 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. Test facility management should ensure that security measures are in place [8].

Responsibilities for computerised systems should be defined and described in policies and procedures. It should be ensured that established standards are met for all phases of the validation. The test facility management usually nominates a validation director and may delegate responsibilities to a system owner.

The **validation director** (VD) is responsible for the overall conduct of the validation of the computerised system.

The **system owner** (SO), if designated by the test facility management, is responsible for ensuring that the computerised system is operated and maintained according to the Principles of GLP and maintained in a validated state.

The **business process owner**, if designated by test facility management represents the user of the computerised system and is responsible for defining the user requirements.

The **personnel** (e.g., laboratory or IT personnel) are responsible for performing activities with computerised systems in accordance with the GLP Principles and recognised technical standards.

The **Quality Assurance (QA)** should verify the validation documentation and inspect the validation activities for GLP compliance.

The following table gives an overview of the validation records and the corresponding roles and responsibilities.

Table 2: Overview

Document	Roles	Responsibilities/Activities
User Requirement Specifications	System owner or Business process owner	Listing all appropriate user requirements that reflect the intended use of the system
Validation plan	Validation director	Overall responsibility for conducting the validation according to GLP, approval of validation plan
	Test facility management	Designates the validation director, signs the validation plan
	Quality assurance inspector	Documented verification of validation plan
Validation plan amendments	Validation director	Amendments to validation plan (e.g., test plan if not included in the validation plan)
	Quality assurance inspector	Documented verification of validation plan amendments

Document	Roles	Responsibilities/Activities
Test raw data	Validation personnel	Conduct of tests and documentation of test results and deviations if they occur.
Validation report	Validation director	Overall responsibility for conducting the validation according to GLP, approval of validation report Statement of compliance
	Quality assurance inspector	Inspection of validation report QA statement
Validation report amendment	Validation director	Amendments to validation report
	Quality assurance inspector	Inspection of amendments to validation report
System release	Test facility management/System owner	Release of the system for productive use

The history of each individual document should be traceable, and changes should be justified.

7 VALIDATION PLAN

The validation plan should describe the validation activities and responsibilities during IQ, OQ and PQ and should be approved before testing.

IQ and/or OQ can be performed and documented by the supplier using defined protocols, procedures and tests. In this case, the validation plan should include the activities planned in these two phases.

The following topics should be covered by the validation plan. Certain aspects may be detailed in separate documents and referenced in the validation plan.

Purpose The purpose of the validation should be stated.

Scope The scope of the validation plan should describe which systems are covered and what is the relation to other connected systems. The boundaries of the system should be defined so that it is clear what is part and what is not part of the system being validated.

Responsibilities The responsibilities for validation related activities associated with the system should be defined according to Table 2.

System description The system description provides an overview of the system and of what the system is supposed to do. The main system functions should be specified. The system should be summarised in terms of hardware, operating environment and software components including cloud services, if applicable. Description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, measures to ensure the integrity of the data, any hardware and software prerequisites, and security measures should be available.

Test environment	If a test environment is used, it should be representative for the laboratory or production environment. Hardware and software components, including cloud services if applicable, should be specified.
Testing	The testing approach should be defined in the validation plan.
Procedure	Guidance should be provided for the change control during validation, the conduct of the tests, the evaluation of the results as well as the contents of the report, if not already defined in the validation policy/SOPs.
Archiving	A list of validation related records to be retained should be given.

8 TESTING

The purpose of testing activities such as installation testing or user acceptance testing is to ensure that the computerised system meets the pre-defined requirements. Testing is in the responsibility of the test facility management [3]. It is advisable to scale the test efforts based on the outcome of the risk assessment. Aspects of the system which are associated with a high risk should receive more attention and be challenged more thoroughly during OQ and PQ testing than aspects associated with a lower risk (see section 5.3).

Testing should follow a pre-defined plan which encompasses test cases and corresponding test scripts. The test cases for the IQ, OQ, PQ are designed to reflect the requirements. Therefore, it is necessary to consider both common and exceptional scenarios. It is important that the requirements and potential failure modes of the system are sufficiently covered. The test scripts should provide detailed step-by-step instructions for testing the test cases. The link between the test cases (and associated test scripts) and the requirements defined in the specifications (design specifications (if relevant) functional specifications and user requirement specifications) should be documented (e.g., in a traceability matrix).

When possible, test cases can be outlined in the validation plan. However, the test cases and test scripts may also be described in separate documents, which should be version-controlled and approved by the validation director prior to being executed.

Testing conducted by the supplier should also be based on predefined requirements and processes which should be documented. The testing approach by the supplier as well as the test results and test documentation should be evaluated by the test facility.

The type of results expected from the tests as well as the acceptance criteria for all qualification phases should be defined prior to testing.

Testing should be conducted based on a test plan. Any deviation from that plan should be recorded and evaluated with regard to the outcome of the validation. As for a GLP study, all data generated should be recorded according to the ALCOA+ criteria (see OECD Document No. 22 [5]) directly, promptly, accurately and legibly by the person generating the data. The procedure for recording test results as well as failures or errors should be specified, e.g., screen shots, log files, printouts. As the test results are considered as raw data, they should be handled and retained in compliance with

the GLP Principles. The raw data should enable complete traceability of the test results.

Based on the test results, fulfilment of the acceptance criteria and requirements is evaluated and reported in the validation report (see next section). If changes to the systems are necessary based on the test results, these should be handled according to the change control procedures. This may include retesting, if necessary (see section 2.2 in [3]).

9 VALIDATION REPORT

The validation report should summarise the validation activities and all test results and conclude whether the system has fulfilled all requirements for its intended use. The validation director signs the GLP compliance statement confirming that the validation complies with the Principles of GLP. The QA should prepare and sign the QA statement confirming that the validation report reflects the raw data. Further responsibilities are shown in Table 2.

The following items need to be addressed in the validation report:

- Summary
- GLP compliance statement
- Quality Assurance statement
- Purpose
- Scope
- System description
- Facilities, personnel and responsibilities
- Validation activities and deviations from the validation plan
- Results of tests and deviations from expected results
- Discussion and conclusion including any system limitations
- Archiving: Storage location of validation documentation

10 SYSTEM RELEASE

Based on the conclusion of the validation report, the test facility management releases the system by signing the validation report or by issuing a separate release document. The test facility management can delegate system release to the system owner. System specific SOPs need to be effective prior to use.

11 ADDITIONAL DOCUMENTATION

In addition to the records generated during the validation, the following documentation is required.

11.1 Inventory of GLP-relevant Computerised Systems

According to OECD Document No. 17, there should be a listing (“inventory”) of all GLP-relevant computerised systems and their functionalities (see [3]), which needs to be updated.

11.2 Standard Operating Procedures

OECD Document No. 17 requires a set of SOPs for the development, validation and/or routine use of validated computerised systems addressing the topics listed below [3].

These SOPs may be generic covering all systems in a test facility (e.g. validation) or specific to a system (e.g. operation).

Validation	SOP describing the validation framework (see Chapter 5.1).
Operation	In addition to the user manual, an SOP should describe how the computerised system will be used for its intended purpose.
Data review	Procedures for data review and audit trail review should be available before start of operation of the system.
Maintenance	Regular and preventive maintenance should be described.
Security	An IT security concept should be defined (OECD Documents No. 17, 22, 25 [3,5,8]) which should include: • Physical security of the system (e.g., locked server room). • Logical security of the system (e.g., UserID, password) including user administration
Incident management	This should describe measures how to document and solve problems encountered during routine operation of the system. Change management procedures (e.g. SOPs) should be considered.
Change control	Changes to the computerised system should be evaluated for their potential impact on the validation status. This may include release management, for example supplier releases of cloud-hosted systems. The procedure how to perform a change control should be described, see also AGIT Guidelines for Change Management and Risk Assessment of Validated Computerised Systems in a GLP Environment [7].
Backup and restore	Procedures for backup of the application and data should be defined including their frequency, period of retention for backup copies, the method and responsibility for periodic backups, and the process of restoration. Backup and restore processes should be implemented and tested.
Periodic review	Procedures for periodic review to ensure that the systems remain in a validated state.
Software development	Procedures for internal software development (e.g. versioning) and respective documentation should be defined.
Contingency plan and disaster recovery	A contingency plan should specify procedures to be followed in case of system breakdown or failure. A

	detailed plan for disaster recovery should be available. Tests should be carried out and results thereof should be documented.
Archiving and retrieval	Procedures should describe how and where documents, software and data are archived, including the period of retention, retrieval mechanism, readability and storage conditions.
Quality Assurance	Procedures how QA will review and inspect the system life cycle and the IT-infrastructure in a GLP-regulated environment.
Data governance	The SOP should describe how the data generated by the computerised system should be handled in order to preserve their integrity during their life cycle (see OECD Document No. 22 [5]).

11.3 System Documentation

Installation manual	A set of instructions that have to be followed when the system is installed. In addition, it defines the minimum hardware and operating system requirements.
User manual	Describes how to use the system, usually provided by the supplier.
Release notes	Contain information on changes and improvements of the software compared to a previous version.
Supplier audit report	Describes the results of the audit of the supplier's processes and quality system.
Source Code	The test facility should have access to the source code of customised systems. For commercial software see [3].

12 ARCHIVING

The validation documentation should be archived according to the OECD GLP Principles and the OECD Document No. 15 [2, 9].

The documents to be archived should be indicated in the validation plan. The validation report should state the location where and in which format (paper or electronically) these documents are stored, if not already addressed in an SOP.

It is necessary to consider long-term retention for all electronic documentation. Specifications are given in the AGIT *Guidelines on the Archiving of Electronic Raw Data* [10].

13 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. 17 Supplement 1: *Advisory Document on GLP & Cloud Computing*, OECD Publishing, Paris, 2023. (OECD)

[5] 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)

[6] Pharmaceutical Inspection Co-operation Scheme (PIC/S): *Good Practices for Computerised Systems in Regulated "GXP" Environments (PI 011-3),* Sept 2007 (PIC/S)

[7] Working Group on Information Technology (AGIT): *Guidelines for Change Management and Risk Assessment of Validated Computerised Systems in a GLP Environment.* (AGIT)

[8] 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)

[9] OECD Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring, No. 15: *Advisory Document of the Working Group on Good Laboratory Practice. Establishment and Control of Archives that Operate in Compliance with the Principles of GLP,* OECD Publishing, Paris, 2007. (OECD)

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

14 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).