GOOD LABORATORY PRACTICE (GLP)

GUIDELINES

FOR THE VALIDATION

OF COMPUTERISED SYSTEMS

Working Group on
Information Technology (AGIT)

Release Date: 14 December 2007

Version: 02

TABLE OF CONTENTS

1 FOREWORD

The aim of this document is to provide guidance on the GLP-compliant validation of computerised systems. It specifies more precisely the procedures to follow in carrying out validations of computerised systems. It intends to help test facilities to promote a common standard to be used. However, the test facility management may use different approaches, as long as they are in compliance with the OECD Principles of Good Laboratory Practice [1]. The extent of a validation may vary depending on the complexity of the computerised system. In any case the validation should demonstrate that the computerised system is suitable for its intended purpose.

The AGIT (Arbeitsgruppe Informations-Technologie) is a working group consisting of representatives from Swiss industry and Swiss GLP monitoring authorities with the aim of proposing procedures, which are practical for use in test facilities fulfilling GLP regulatory requirements. These guidelines have been adapted to current practices and replace those issued in June 2000.

2 REGULATORY REQUIREMENTS

The validation of computerised systems is required by the OECD Principles of Good Laboratory Practice [1]. A more detailed description of the application of the principles of GLP to computerised systems was already published in OECD GLP consensus document No.10 [2]. This document specifies what is needed for the life cycle of computerised systems in a GLP regulated environment.

The OECD GLP Principles and OECD Consensus document No.10 define validation as *"The demonstration that a computerised system is suitable for its intended purpose"*. The validation process provides a high degree of assurance that a computerised system meets its pre-determined specifications.

The present document is an interpretation of the OECD GLP Principles regarding computerised systems and the corresponding consensus document and gives guidance for practical implementation of these principles to computerised systems in a GLP environment with specific regard to validation.

3 COMPUTERISED SYSTEMS

3.1 Definition

Computerised systems can vary from a programmable analytical instrument or a personal computer to a Laboratory Information Management System (LIMS) with multiple functions. *"Whatever the scale of computer involvement, the GLP Principles should be applied"* [2]. Consequently, 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 complexity of a system the extent of testing and documentation may strongly differ.

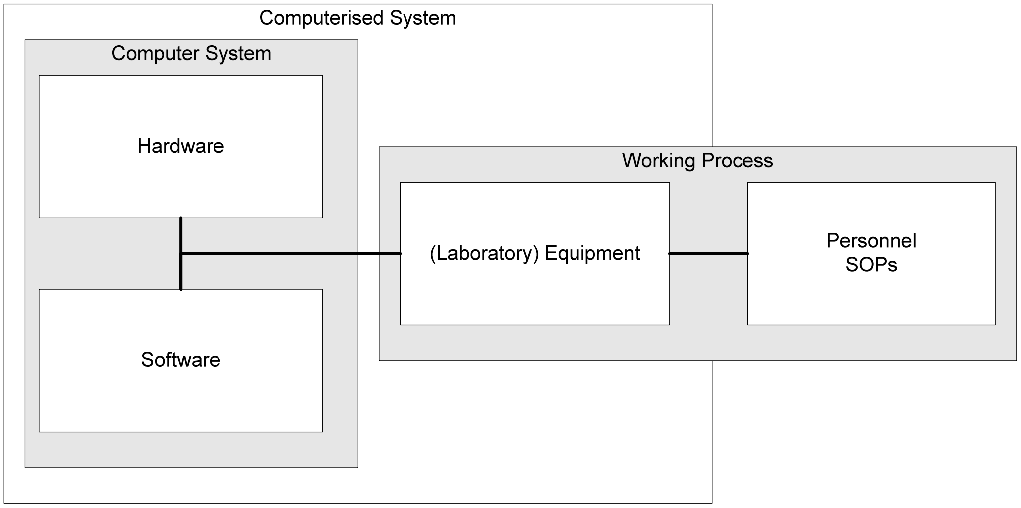


Figure 1: Definition of a Computerised System

A general accepted model of a computerised system is depicted in Figure 1. A computerised system in a GLP environment consists of computer hardware and software, which forms the computer system. Laboratory equipment is connected or integrated with this computer system and together with the personnel, SOPs, training etc. makes up the working process. This model describes a vast range of possible systems. The computer system in a LIMS will be more complex (server, network, terminals etc.) than for a laboratory instrument connected to a standalone PC.

Before validation the boundaries of a computerised system should be clearly defined. Because the validation of a laboratory instrument as an integral part of a LIMS is more 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.

3.2 Which systems should be validated?

"All computerised systems used for the generation, measurement or assessment of data intended for regulatory submission should be developed, validated, operated and maintained in ways which are compliant with the GLP Principles" [2]. Computerised systems delivering supporting data (e.g. temperature and humidity) for GLP studies should also be considered.

Computerised systems should be validated if they are involved in the process of generation, measurement or assessment of data, and if instrument calibration alone is not sufficient to prove the functionality and reliability of the system.

For example, calibration of a stand-alone balance measuring body weights (weights recorded on paper) is sufficient. However, if the balance is part of a LIMS or if the weights can be modified before they are printed to paper, the process of data acquisition and further processing should be validated. Since this decision should be taken for each individual computerised system it may be helpful to define categories of instruments/systems with the corresponding assignment to a validation process or function control tests in an SOP. An example of system categories is given in Appendix 1.

Before a system is bought or developed it is recommended that a high level risk assessment be performed in order to assess the GLP relevance of the system. The decision whether a system is GLP relevant and a validation is needed should be documented. The following questions may guide the decision process:

- 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 should be validated.

3.3 Critical issues

It is not reasonable to validate an operating system (e.g. Windows, UNIX, LINUX) as such at the user site. The functionality of the operating system is implicitly validated during the course of the validation of a computerised system (application).

This is also the case for databases and framework packages such as Oracle, SAS, and Excel. However, user applications written within or by means of these packages, such as SAS procedures, ORACLE applications, and Excel spreadsheets (including complex calculations and macros) should be validated. If such user applications are not validated, a documented quality control of the generated data is necessary.

Software applications such as LIMS (e.g. Watson, PathData) with functionalities tailored to the user requirements should be validated. Operating systems and databases as described above, which form an integral part of the software applications, are thereby indirectly validated.

4 VALIDATION PROCESS

4.1 Validation Policy

According to OECD GLP Consensus document No. 10 there should be a management policy for validation. This validation policy establishes the principles for performing the validation of computerised systems in compliance with the OECD GLP Principles. It is recommended that this policy should cover and define all general validation aspects for the entire life cycle of computerised systems.

While a validation policy defines the general principles of validation to be followed within a company, documents (e.g. validation master plan, SOPs) should be set up, which are dedicated to a particular system or group of systems describing the entire life cycle of the system from the point of user requirement definition to system retirement. These documents can be regarded as planning tools covering all aspects of the validation of a particular computerised system or for a category of systems during the full life cycle.

4.2 Validation Strategy

The GLP principles allow some flexibility in carrying out validations. For many reasons it seems reasonable to conduct the validation formally in a similar way as for an experimental study. The GLP principles are quite precise with regard to the specifications of study plan, conduct of a study, reporting of study results, storage and retention of records. Furthermore, they require the assignment of responsibilities and the availability of standard operating procedures. All these principles can conveniently be applied to computerised system validation (CSV). Therefore, it is recommended that validations be carried out in a way analogous to GLP studies. This will guarantee compliance with the principles of GLP and facilitate the general understanding of the procedures by the parties involved.

GLP Study	CSV	Remarks
Study Director (SD)	Validation Director (VD)	Ultimate responsibility
Study plan	Validation plan	Approved by SD/VD
Method description	Test scripts	Referenced to or included in plan
Conduct of study	Conduct of testing	Process executed according to the validation plan and test scripts
Raw data	Validation raw data	Documented evidence of test results
Study report	Validation report	Audited by QA and signed by SD/VD

Table 1: Computerised System Validation analogies to a GLP Study

In any case a validation should be carried out at the user’s site with the local computerised system. A validation performed at the vendor’s site is not sufficient. However, in order to make use of synergies, where appropriate, test plans provided by the vendor, test scripts or checklists may be used for validations at different locations adapted to the specific situation.

4.3 System Life Cycle

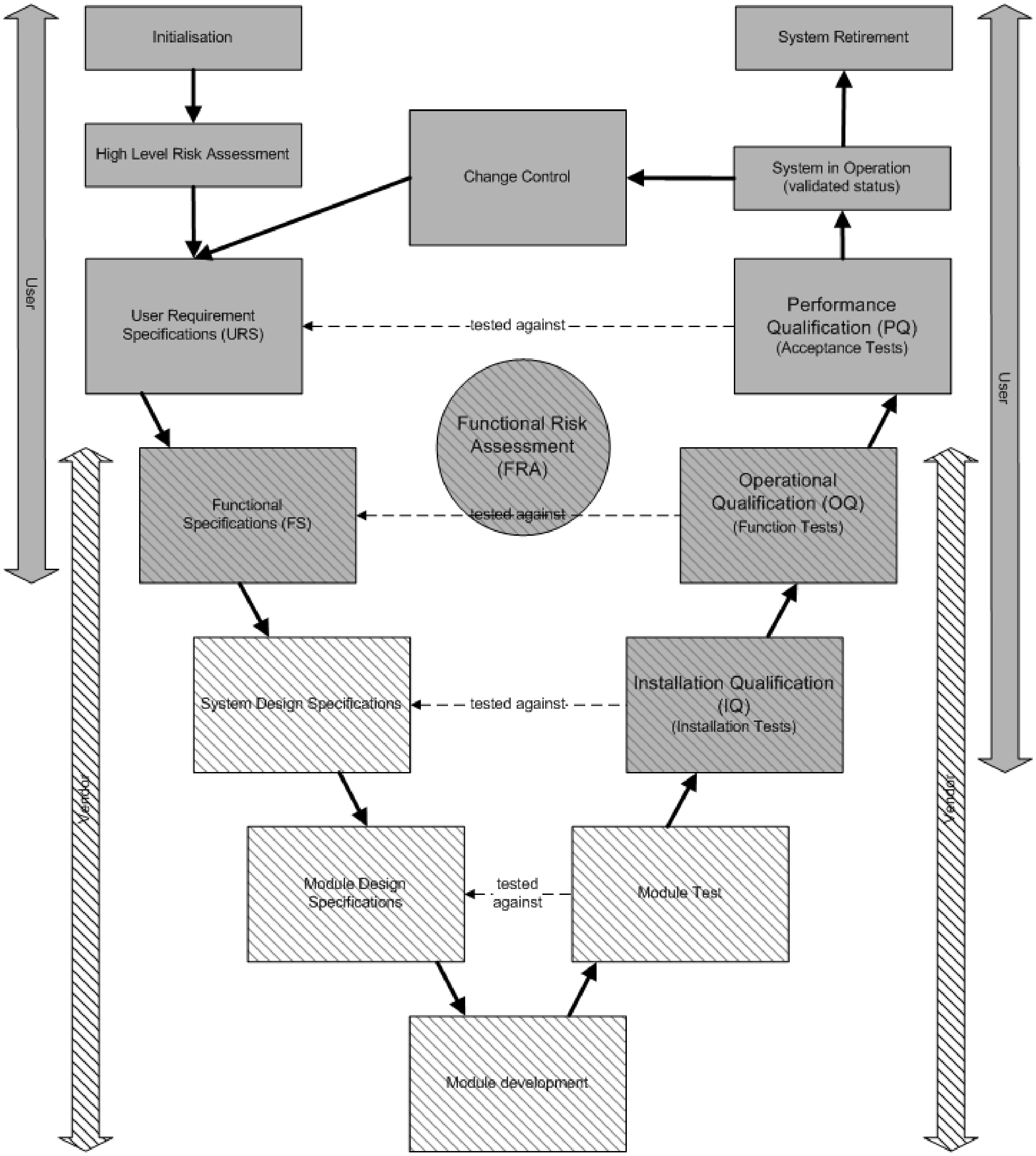
A generally accepted life cycle of a computerised system is the V-model as shown in Figure 2. This model gives an overview of the different phases during a system development life cycle.

Initialisation and High Level Risk Assessment

Prior to the acquisition of a commercially available system or development of a custom-built computerised system, the potential users define the specific tasks for which the computerised system will be used. The decision whether a system is GLP relevant and a validation is needed should be evaluated at this point by means of a high level risk assessment as described in chapter 3.2.

User Requirement Specifications (URS)

The users formally compile all requirements in a document called user requirement specifications**.** These user requirements contain scientific, business, regulatory, safety, performance and quality aspects of the future system. During the process of defining the user requirement specifications it is necessary to differentiate between essential and desirable requirements. The essential requirements for the intended purpose should be unequivocal and testable. It is of paramount importance to realise that the user requirements serve as the basis for the User Acceptance Testing, also referred to as Performance Qualification (PQ).


Initialisation
High Level Risk Assessment
User Requirement Specifications (URS)
Change Control
System Retirement
System in Operation (validated status)
Performance Qualification (PQ) (Acceptance Tests)
-tested against-
Functional Risk Assessment (FRA)
Functional Specifications (FS)
tested against
Operational Qualification (OQ) (Function Tests)
System Design Specifications
tested against
Installation Qualification (IQ) (Installation Tests)
Module Design Specifications
tested against
Module Test
Module development
User
User
Vendor
Vendor

The processes in the shaded boxes can be performed by the vendor or by the vendor in cooperation with the user

Figure 2: The V-model describes the system development life cycle

Functional Specifications (FS)

The next level concerns the functional specifications (FS) of the computerised system. In case of a custom-built system, the vendor (in cooperation with the user, if applicable) translates the user requirements into functional specifications. However, if the user prefers to purchase a commercially available product, the functional specifications have been predefined by the vendor and therefore the user should compare the offered functionality of the product with the user requirements and determine whether the product could in principle fulfil the user's needs.

System Design Specifications (DS)

The system design specifications define all the necessary system components: 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 vendor. Thus, the user is not directly involved, but should ensure that the system was developed according to commonly accepted standards, e.g. by a (vendor) audit.

Installation Qualification (IQ)

Installation Qualification (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 vendor in cooperation with the user, if applicable.

Functional Risk Assessment (FRA)

Generally, 20% of system functions cover 80% of the functional needs in daily use. Therefore, testing of all the system functions in the Operational Qualification (OQ) phase is not deemed necessary. It is recommended that a risk assessment of the functional specifications be performed. This functional risk assessment shows which functions are essential and important for the intended use of the computerised system. The extent of OQ testing for each function is based on the outcome of the functional risk assessment.

Operational Qualification (OQ)

Operational qualification has the aim of demonstrating that all functions needed for the intended purpose are available and operate reliably in the user's environment. This additional qualification at the user's site can be performed by the vendor and/or user, if applicable.

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

Performance Qualification (PQ)

The aim of the performance qualification is to demonstrate that a computerised system is suitable for its intended purpose in the user's own environment as defined in the URS. The user requirements should be tested in the PQ phase to cover the overall business use (use cases) of the system in the daily routine.

System in Operation

After successful completion of all qualification phases, including its 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 must ensure that all personnel operating the system are trained and that the necessary SOPs are in place.

Change Control
Any change to the system during its operational use should be performed in a controlled manner to maintain its validated state (see Chapter 12).

System Retirement
After termination of its productive use, the system should be formally retired. The retirement process is described in more detail in Chapter 13.

4.4 Vendor Audit

The user of computerised systems should make sure that the system was developed in compliance with a defined quality standard. For vendor-supplied systems it is likely that much of the design, test and quality documentation created during the development is retained at the vendor's site. In this case, evidence of a formal assessment (e.g. a vendor audit report) should be available at the test facility [2].

5 RESPONSIBILITIES AND DOCUMENTS

The responsibilities for a validation are extensively described in OECD GLP consensus document No. 10. The main responsibilities can be summarised as follows:

The **management** of the test facility has overall responsibility for compliance with the GLP principles. In particular it 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. Responsibilities for computerised systems must be defined and described in policies and procedures. It should be ensured that established standards are met for all phases of validation. The test facility management has to designate the validation director and the system owner.

The **validation director** is responsible for the overall conduct of the validation.

The **system owner**, 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 **personnel** are responsible for performing activities with computerised systems in accordance with the GLP Principles and recognised technical standards.

The **Quality Assurance (QA)** has to review the validation documentation and inspect the validation activities for GLP compliance.

The following table gives an overview of the responsibilities, the relevant documents of a validation and the persons who should sign the corresponding documents.

Document	Responsible persons	Signature	Responsibilities/Activities
User Requirement Specification	System owner	mandatory	Listing all appropriate user requirements that reflect the intended use of the system
Validation plan	Validation director	mandatory	Overall responsibility for conducting the validation according to GLP, approval of validation plan
	Test facility management	optional	Recommended for designation of the validation director
	System owner	optional	Responsibility for the system
	Person responsible for IT	optional	IT infrastructure support
	Quality assurance inspector	optional	Documented verification of validation plan
Validation plan amendments	Validation director	mandatory	Amendments to validation plan (e.g. test plan if not included in the validation plan)
	Quality assurance inspector	optional	Documented verification of validation plan amendments
Test raw data	Validation personnel	mandatory (minimally initials)	Conduct of tests and documentation of test results and deviations if they occur.
Validation report	Validation director	mandatory	Overall responsibility for conducting the validation according to GLP, approval of validation report
	System owner	optional	Responsibility for the system
	Person responsible for IT	optional	IT infrastructure support
	Quality assurance inspector	optional	Inspection of validation report
GLP statement [1)]	Validation director	mandatory	Overall responsibility for compliance with GLP
QA statement [1)]	Quality assurance inspector	mandatory	Assurance of the GLP compliant conduction of the validation: provides dates of review of validation documentation and inspections
Validation report amendment	Validation director	mandatory	Amendments to validation report
	Quality assurance inspector	optional	Inspection of amendments to validation report
System release	Test facility management/system owner	mandatory	Release of the system for productive use.

1) Part of validation report or validation report amendment

Table 2: Responsibilities/activities and documents for validation

6 VALIDATION PLAN

The validation plan should be an approved document, which describes the validation activities and responsibilities during IQ, OQ and PQ. The validation plan should be in the form of a study plan and should be prepared and approved prior to conducting the tests.

IQ and/or OQ can be performed and documented by the vendor using his own protocols, procedures and tests. In this case, the validation plan refers to these two phases and should be issued and approved prior to starting the PQ.

The following topics should be covered by the validation plan:

Purpose The validation should provide documented evidence that the computerised system is suitable for its intended use.

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 and what is not included as part of the system being validated. Furthermore, it should be indicated where the system will be located.

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

System description The system description is to provide an introduction to the system showing what the system is supposed to do and in what environment it will be operated. The main system functions should be specified. The system must be summarised in terms of hardware and software components.

Test environment Hardware and software components should be specified for the test environment if it is not the productive environment.

Tests Based on the respective requirements (DS, FS, URS), test cases for the IQ, OQ, PQ and their underlying test scripts should be defined. On the level of FS/OQ, the functional risk assessment (FRA) should be considered, wherein system functions have been individually analysed for the likelihood and consequences of failure. Functions deemed “high risk” should be challenged thoroughly during OQ. The expected results as well as the acceptance criteria for all qualification phases should be defined.

If possible, test cases should be defined in the validation plan. However, the test scripts may be handled in one or several separate documents. Their versions should be indexed and approved by the validation director. The history of each individual document should be traceable and changes should be justified.

The error logging procedure should be specified as well as the procedure for documentation of the test results, e.g. screen shots, log files, printouts. Since the test results are considered as raw data, their generation and the handling of these data should be in compliance with the GLP principles.

Procedure Guidance should be provided for 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.

Documentation An index of all documentation relating to the computerised system, including but not limited to SOPs, user developed documentation, and vendor/provider developed documentation should be provided. For details see Chapter 9.

Archiving A list of records to be retained should be given.

7 VALIDATION REPORT

The validation report summarises all test results and presents a conclusion whether the system has fulfilled all requirements for its intended use.

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

- Summary
- Release approval (could be in a separate document)
- GLP compliance statement
- Quality Assurance statement
- Purpose
- Scope
- System description
- Facilities, personnel and responsibilities
- Validation method and deviations from it
- Results of tests and deviations from expected results
- Discussion and conclusion including any system limitations
- Archiving

The validation director is responsible for the GLP compliant conduct of the validation; thus, he should sign the GLP compliance statement. Quality Assurance should inspect the validation report. 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.

8 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.

9 DOCUMENTATION

In addition to the validation documentation that has already been described, the following documents should be available:

9.1 Basic Documentation

In addition to the basic GLP documentation (i.e. training record, job description, and CV), there should be an inventory of all computerised systems being used in the facility listing system name, system owner, location and validation status.

9.2 Standard Operating Procedures

OECD GLP Consensus Document #10 requires a set of standard operating procedures for the development and/or routine use of validated computerised systems addressing the following topics:

Operation
In addition to the User Manual, an SOP should describe how the computerised system will be used for its intended purpose.

Security
Two levels of security should be addressed:

Physical security of the system (e.g. locked server room).

Logical security of the system (e.g. UserID, password) including user rights.

Problem log
This should describe measures how to document and solve problems encountered during routine operation of the system. Reference to change management procedures should be taken into account.

Maintenance
Regular and preventive maintenance should be described.

Change control
Changes to the computerised system, except regular and preventive maintenance, should be evaluated for their potential impact on the validation status. The procedure how to perform a change control should be described.

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.

Periodic testing
The system needs to be monitored regularly for correct operation including device checks. Basic functionality testing should be performed on a regular basis.

Software development
If software is developed by the user or an internal IT group, standards for software design, coding, testing and versioning should be defined and should refer to a commonly acknowledged software development life cycle model.

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.

Apart from the SOP on operation of a system, these SOPs may be as generic as possible; i.e. they need not be written separately for each application.

9.3 Additional System Specific Documents

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 vendor.

Release notes
Contain information on changes and enhancements of the software compared to a previous version.

Vendor audit report
Describes the results of the inspection of the vendor concerning the software development life cycle (SDLC) and the quality system of the vendor. It also includes information about software design and, in particular, about software testing.

Logbook
Should be established to record all actions e.g. calibration, cleaning, maintenance, change control of all components of a computerised system over the whole life cycle.

Source Code
The test facility should have access to the source code of application software. It is not necessary to have it available at the test facility, but the test facility should ensure that the vendor of the software maintains the source code for each version in a safe place.

10 ARCHIVING

The validation documentation should be archived according to the OECD GLP Principles and the corresponding advisory document [3].

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.

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 [4].

11 RETROSPECTIVE EVALUATION

For the validation of systems, which were originally not foreseen or not specified for GLP use, it is necessary to perform a retrospective evaluation. Retrospective evaluation begins with gathering all historical records related to the computerised system. These records are then reviewed and a summary is produced. This retrospective evaluation summary should specify what validation evidence is available and what still needs to be done to ensure the suitability of the system for its intended purpose.

Furthermore a complete collection of all available system documentation should be assembled. In particular a description of the system, system specifications, manuals for system managers and users and the availability of the source code should be specified. The quality and completeness of this documentation should be assessed.

Based on the available documentation a risk assessment should be carried out to determine whether the available information is sufficient to ensure the suitability of the system for its intended purpose or whether tests or a validation is necessary. The tests or validation should be performed as described in this document. Reasons for using the selected procedure should be given. The retrospective evaluation, the results of the risk assessment and the measures taken should be documented.

12 CHANGE CONTROL

Effective change management is an important factor for maintaining a productive computerised system in a validated state. A change request must be formally approved by the system owner and documented. This includes application software updates, operating system updates, changes to the hardware and changes to laboratory equipment.

The risk of the change should be assessed for its potential impact on the performance of the computerised system. The risk assessment should be documented and reasons for the decision should be given. Based on such a risk assessment and depending on the extent of changes of the system either complete, partial or no testing should be performed. If necessary, user requirement and functional specifications and the corresponding OQ and PQ test scripts should be updated accordingly (see fig. 2).

In an emergency case (e.g. hardware crash), an immediate change may be required to bring the system back into operational use. Based on an informal risk assessment by the system owner and the personnel involved (e.g. IT), the necessary changes can be implemented immediately. However, the formal change control procedures (approval, documentation, testing) should be performed retrospectively.

After successful completion of the change, the system can be released for operational use by the test facility management or the system owner.

13 SYSTEM RETIREMENT

At the end of the system life cycle, the system should be retired. The retirement should be performed according to a formal system retirement plan and documented in a report approved by the test facility management or the system owner. The entire system documentation (log books, system manuals etc. in paper or electronic form) and the software applications should be archived. The retirement of the system may have an impact on the accessibility and readability of the archived electronic raw data generated by the system. For details see [3, 4].

14 REFERENCES

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

[2] OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 10: GLP Consensus Document. The Application of the Principles of GLP to Computerised Systems. Environment Monograph No. 116; Environment Directorate, OECD, Paris, 1995

[3] OECD Advisory Document of the Working Group on GLP: Establishment and Control of Archives that Operate in Compliance with the Principles of GLP. Paris 2007

[4] Working Group on Information Technology (AGIT); Good Laboratory Practice (GLP); Guidelines for the Archiving of Electronic Raw Data in a GLP Environment. *Qual Assur J* 2003; **7**: 262-269.

Appendix 1: Example of system categories

Category A:		**Exempted Systems**
	Definition	No calibration function Framework/layered software
	Examples	Calculator, microscope, photo or video camera, standard office PC, Microwave, etc. Operating system (e.g. Windows, Linux, Unix) network software, security software (virus check, firewall), application software (Word, Excel), data base software (e.g. Oracle, Access)
	Action	• None
	Documentation	• Inventory list, system description
Category B:		**Simple computerised systems**
	Definition	Small part of software Restricted customisation
	Examples	pH-meter, oxidizer, incubator, titration processor, colorimeter, thermo hygrograph, balance, particle sizer, UV/VIS spectrometer, liquid scintillation counter, TLC analyser, AAS, micro plate counter, image analyser, polarimeter, etc.
	Action	• System SOPs (for use, maintenance, function control test) • Calibration • Function control test
	Documentation	• Logbook / change control log file • User training
Category C:		**Complex computerised systems**
	Definition	Extended amount of functionality software Extended customisation
	Examples	LIMS, automated sample processing systems, liquid chromatograph (LC, HPLC), gas chromatograph (GC) including auto sampler and detection systems (UV, VIS, IR, MS, NMR, radioactivity or fluorescence monitor, etc.), biological analyser, ECG, etc..
	Action	• Validation
	Documentation	• User requirement specification • Risk assessment • Validation plan • Validation raw data • Validation report • System description • Logbook / change control log file • System SOP's (for use, maintenance, function control test) • User education

Working Group on Information Technology (AGIT)

The Working Group on Information Technology (AGIT) was founded on 27 March 1998 with the objective of discussing relevant problems of Good Laboratory Practice (GLP) in the field of information technology between industry and the monitoring authorities.
The AGIT intends to set up guidelines based on legislative requirements and practical experience to support test facilities introducing information technology tools to computerised systems in practice. OECD GLP Consensus Document number 10 on the application of the principles of GLP to computerised systems is used as a basis for the discussions.

The members of the AGIT are representatives of the Swiss GLP monitoring authorities (Gérard Donzé, Swiss Federal Office of Public Health; Roger Zühlke, Swissmedic, Swiss Agency for Therapeutic Products; Hans Peter Saxer, Federal Office for the Environment), and representatives from industry (Peter Esch, Novartis Pharma AG; Bruno Eschbach, PDS Pathology Data Systems AG; Stephan Hassler, RCC Ltd.; Leo Hutter, RCC Ltd; Uwe Timm, F. Hoffmann-La Roche AG).

For the convenience of users, AGIT publications are available on the Swiss GLP home page **www.glp.admin.ch**.

The Swiss GLP home page also provides links and references to guidelines, laws and regulations, definitions, relevant literature, training courses, workshops etc.

AGIT Publications (as of 2007):

- Guidelines for the Validation of Computerised Systems
  (Version 01, June 2000). Replaced by the current version.
- Guidelines for the Management of Electronic SOPs in a GLP Environment
  (Version 01, July 2001)
- Guidelines for the Archiving of Electronic Raw Data in a GLP Environment
  (Version 01, May 2003)
- Guidelines for the Acquisition and Processing of Electronic Raw Data in a GLP Environment
  (Version 01, December 2005)