Good Laboratory Practice

CHANGE MANAGEMENT AND RISK ASSESSMENT OF VALIDATED COMPUTERISED SYSTEMS IN A GLP ENVIRONMENT

Release Date: 31.01.2018

Version: 2.0

TABLE OF CONTENTS

1 FOREWORD

The aim of the present document is to provide guidance on the GLP-compliant change management of validated computerised systems. The guidance will 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 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 Guideline for Change Management and Risk Assessment of Validated Computerised Systems in a GLP Environment was originally issued in December 2012. This updated version (version 2.0) is in line with the OECD Advisory Document No. 17 (replacing OECD Consensus Document No. 10) [3].

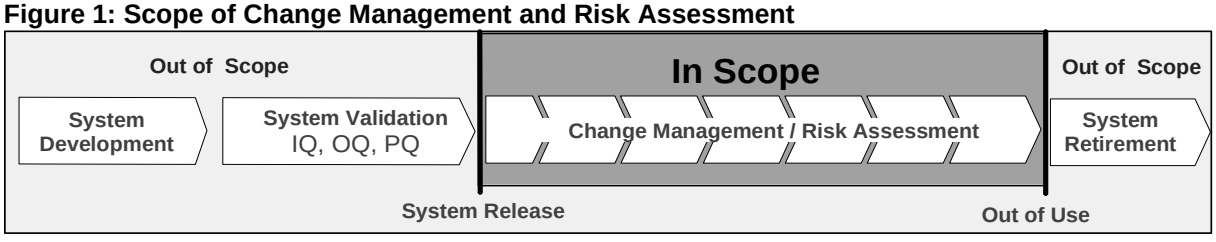
2 INTRODUCTION

The life cycle of validated computerised systems is initiated by the conception and definition of user requirements followed by a documented validation process. After release of the computerised system, a change management process is needed to ensure the validation status throughout the entire system life cycle [3]. Change management requires a controlled process to monitor and document all changes on released systems. Changes should be evaluated with regards to their impact (risk assessment) on the validation status and appropriate measures should be taken to keep the system in a validated state.

3 SCOPE

Computerised systems should be validated prior to use within GLP regulated areas. In order to ensure the validated status of the system, change management principles should be applied until system retirement. The present guidelines describe the change management process of the operational phase and its documentation requirements.

Figure 1: Scope of Change Management and Risk Assessment



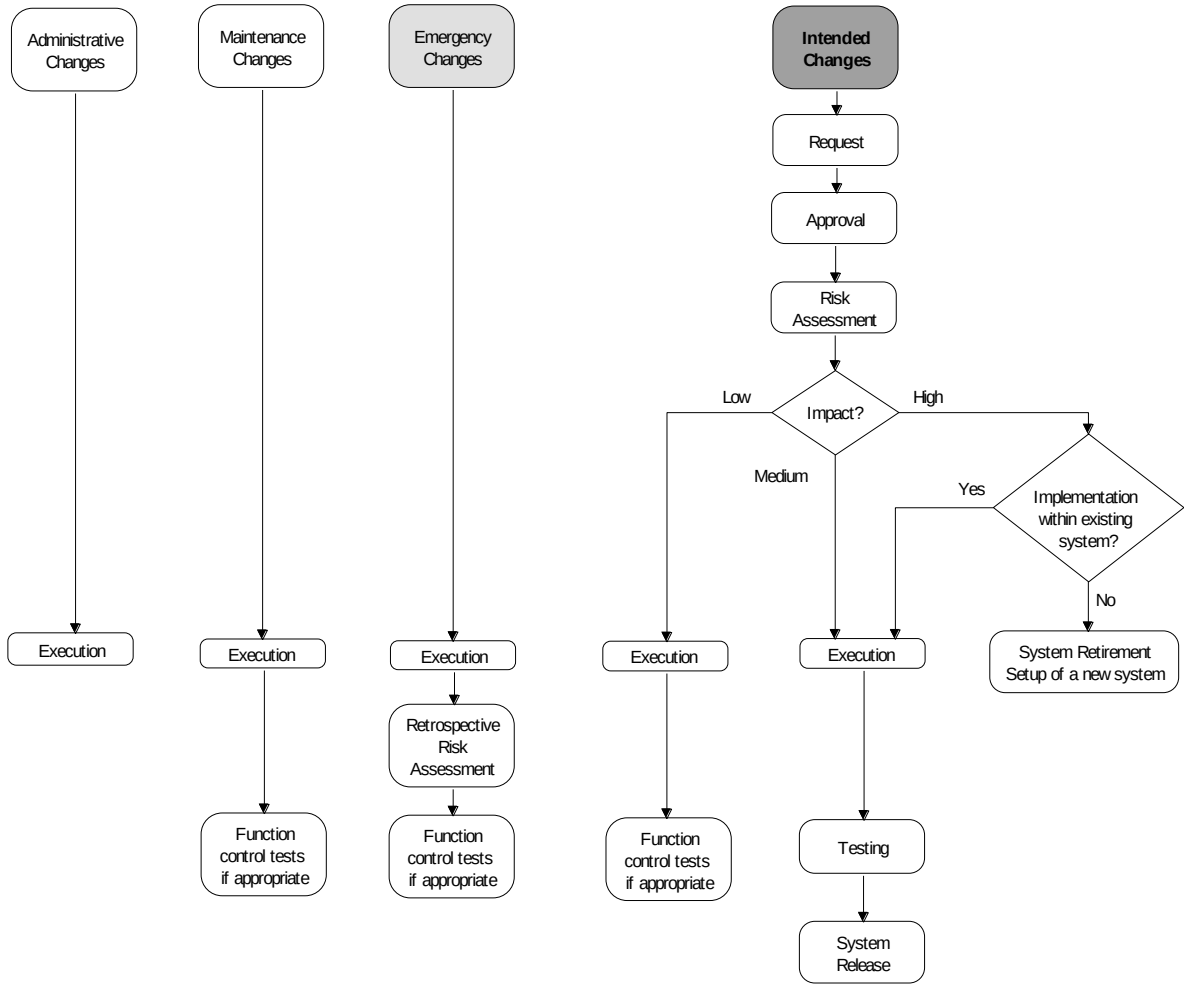
Change management during the system development process and during the system retirement is out of the scope of this guideline (see V-Model of development life cycle [4]).

Information on the system validation process and the system retirement principles can be found in [4, 5] and are not part of this guideline.

4 TYPES OF CHANGES

The different types of changes and their implementation are depicted in figure 2.

Figure 2: Workflow Diagram



4.1 Administrative Changes

Change of roles and responsibilities, e.g. system owner, registered users, should be documented accordingly in the system log book or system log files. The functionality of the computerised system is unaffected, and therefore no further measures are required. However, education and training should be considered, and personnel and/or system documentation should be updated as necessary.

4.2 Maintenance Changes

Replacement of attrition parts may be necessary during regular maintenance of computerised systems. In general these changes do not affect the functionality of the system. The necessary documentation of these changes can be fulfilled by several options, e.g. maintenance report, detailed documentation in log book or log file. In some cases function control tests should be performed to ensure the proper functionality of the system. The hardware components, which fall into the category “attrition parts” should be described in an SOP.

Software upgrades in the context of maintenance should be considered as critical, since the impact of all changes in software should be evaluated. Therefore it is recommended in this case to follow the intended change procedure.

4.3 Emergency Changes

In case of a system failure (e.g. hardware crash), an immediate change may be required to bring the system back into operational use. Based on the given facts the system owner and the personnel involved (e.g. IT) should decide on the necessary changes, which should be implemented immediately to prevent a loss of data integrity. In this case, the formal change control procedures (approval, documentation, testing) should be performed retrospectively. Depending on the results of the retrospective risk assessment or in the event of a negative outcome of the function control tests, remediation should follow the “intended changes” procedure. In this case, the status of the computerised system has to be considered as no longer validated. The system should not be used for GLP studies from the time of the system failure until release.

4.4 Intended Changes

An intended change is a planned upgrade or modification of the system. The detailed procedure is described below.

5 PROCEDURE FOR INTENDED CHANGES

5.1 Request

In case of an intended change, a documented request should be submitted to the system owner. A change may be requested by different parties, e.g. users, IT specialists, quality assurance, vendor, system owner, test facility management.

In order to evaluate the importance of a request the change should be clearly described and include the justification for the change, e.g. improved functionality, added value, corrective measures, as well as the urgency of the change. Additionally, this description should include the elements of the system, which are considered to be affected (hardware, software, interfaces, documentation, as well as training).

In order to support the approval, a preliminary evaluation of the overall effort (amount of effort for testing and documentation) for the implementation of change might be helpful to make the business decision whether the change should be made or not. Prior experience and knowledge should be taken into account. The overall effort may be difficult to predict, especially for changes having a medium or high impact.

5.2 Request Approval/Rejection

Based on the justification for the change and the expected effort, test facility management or the system owner on behalf of test facility management should approve/reject the request. The approval/rejection should be documented. Alternatively the request can be approved/rejected after the risk assessment.

5.3 Risk Assessment

If new or improved functionalities are intended to be used, it is necessary to update the user requirements accordingly.

All affected user requirements/functional specifications should be identified.

For each affected user requirement/functional specification a decision for testing should be taken. This decision should be taken based on technical expertise, possible impact on data integrity, functionality of the system, practical application, and probability of malfunction. The extent of testing should be described in the corresponding test plan/test script. If no testing is decided for an affected user requirement/functional specification a justification should be given.

Example 1: User requirement affected but testing is not required.

The intended change is the recommended upgrade of the software version due to support reasons. One of the differences to the old version is that the new version allows 32 characters instead of 6 in the entry field of study number. The user requirement of 6 characters in not affected and therefore no test is required.

Example 2: User requirements are affected and testing is required

The new version of the software has an improved auto integration functionality (new algorithm). Several user requirements are affected and should be tested.

Operation	User Requirement	User requirement affected	Test required	Justification
	...			
Data processing and evaluation				
4.1	Manual integration function, i.e. set start and end of fraction on graph and on time event table.	No		
4.2	Definition of BG area.	No		
4.3	Smoothing of signal, i.e. 2-10 point smoothing.	Yes	Yes	
4.4	Auto integration based on slope and treshold.	Yes	Yes	
4.5	Batch re-processing of integration based on defined integration methods	Yes	Yes	
	...			

If none of the affected user requirements needs to be tested, this change is considered as a low impact change. As soon as testing of one or more user requirements is required the change is considered as a medium or high impact change. The difference between medium and high impact is the extent of testing necessary.

5.4 Actions Required

If a change has a **low impact** on the computerised system the validation status remains unchanged, but the change and the correct functioning of the computerised system should be documented in the system documentation and/or log book. If appropriate, function control tests should be performed to ensure the proper functionality of the system.

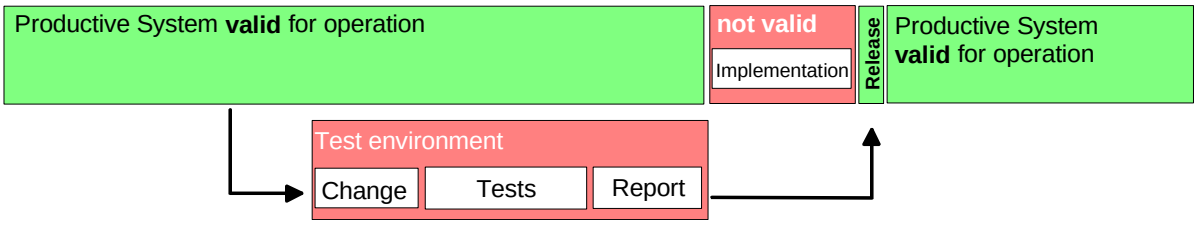
If a change has a **medium/high impact** on the computerised system, the validation status will change to “not validated” as of change execution and the computerised system should therefore not be used for GLP purposes. After identification of all affected user requirements, a test plan (approved by system owner) should be established in order to prove that these user requirements are tested and QA should be involved according to SOP. The defined tests should be executed and reported. Alternatively a function control test, already defined in an SOP, can be used if appropriate. If evidence is given that all tested user requirements are met, the

computerised system is suitable for its intended use. The computerised system can be released by the test facility management/system owner for productive use for GLP studies.

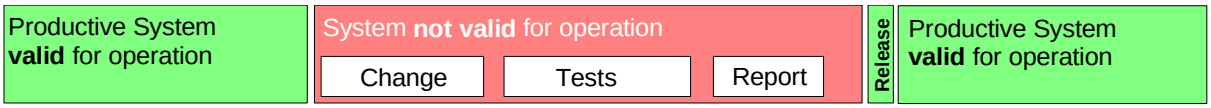
In the case of a **high impact** it may be appropriate to formally retire the current system, define the new system, and initiate a new validation process [4].

5.5 Implementation of Change and Validation Status

For changes with a medium/high impact it should be considered that the computerised system will no longer be valid for productive use as of change execution. It is highly recommended to establish a roll out plan for the change execution. It might be appropriate to perform the planned tests in a test environment of the computerised system while the unchanged productive environment remains valid for operation. After the successful completion of the tests the change should be implemented on the productive computerised system. Appropriate testing in the productive environment may be required prior to system release.



If a test environment is not available, the change should be executed on the productive system. During the change the computerised system cannot be used for GLP studies until released by test facility management/system owner.



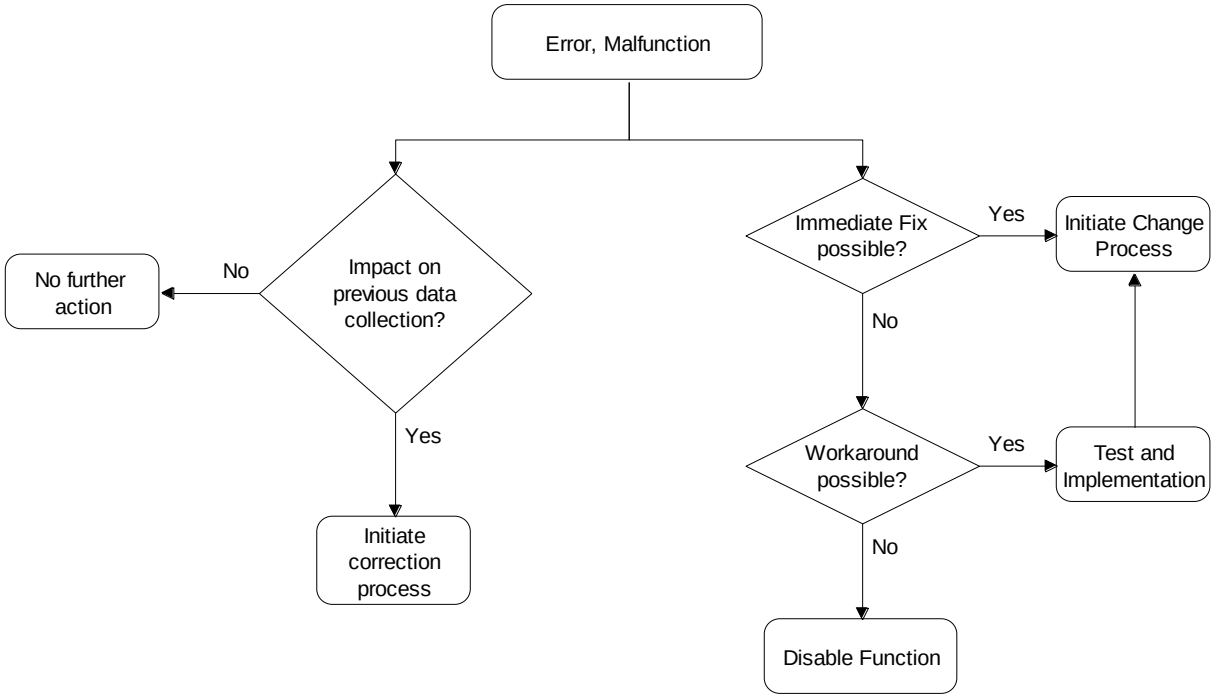
5.6 Close of Change

A low impact change is closed when the system documentation is updated.

In case of a medium/high impact the change is closed with the release of the changed system. Documentation of the change including risk assessment, test plan, test data, test report, implementation, and system release is supplementary to the validation documentation.

6 ERROR HANDLING

Any recognized error or malfunction, during system life cycle should be documented and evaluated according to the following scheme. Both process lines should be executed in parallel, i.e. assessment of impact on existing data and error fixing.



Any possible impact on previous data collection or processing should be assessed by the study director. If there is an impact, a correction of the previous data should be initiated, i.e. information to all involved parties, final report amendment, raw data correction, etc.. If there is no impact on data, then no further action is required. In both cases the outcome of the evaluation process should be documented.

For the further use of the system an immediate correction process should be initiated by an intended change process. If an immediate fix is not possible, a workaround should be established and tested in order to avoid impact on data integrity for ongoing operations. A possible workaround includes technical and/or operational measures. Subsequently the undertaken measures should be communicated to all involved parties, e.g. users, study directors, QA. If no workaround is feasible the corresponding function should be immediately disabled or no longer be used.

7 RESPONSIBILITIES

This section provides a description of the roles and responsibilities for the change management process.

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. This responsibility may be delegated to a designated system owner.

The **system owner** is responsible for ensuring that a particular computerised system is operated and maintained according to the Principles of GLP and maintained in a validated state.

The **study director** has the responsibility to ensure that all computerised systems used in the studies are validated and used appropriately.

The **personnel** involved in executing tests are responsible for performing activities in accordance with the GLP Principles and recognised technical standards.

The **Quality Assurance (QA)** should be integrated in the change management process. The QA involvement should be described in an SOP. The following topics should be addressed:

- Information process on planned activities
- Review of documents (e.g. test plan, test report)
- Inspection of activities.

8 REFERENCES

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

[2] 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. (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. Environment Directorate, OECD, Paris, 2016. (OECD)

[4] Working Group on Information Technology (AGIT): Good Laboratory Practice (GLP); Guidelines for the Validation of Computerised Systems. (AGIT)

[5] Working Group on Information Technology (AGIT): Good Laboratory Practice (GLP); Guidelines for Archiving of Electronic Raw Data in a GLP Environment. (AGIT)

9 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 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 Advisory Document number 17 on the *Application of the Principles of GLP to Computerised Systems* is used as a basis for discussion.

The members of the AGIT are representatives of the Swiss GLP monitoring authorities (Olivier Depallens, Swiss Federal Office of Public Health; Elisabeth Klenke and Daniel Roth, Swissmedic, Swiss Agency for Therapeutic Products; Christoph Moor, Federal Office for the Environment), and invited experts from industry (Peter Esch, Novartis Pharma AG; Stephan Hassler, Innovative Environmental Sciences Ltd.; Silvio Albertini, F. Hoffmann-La Roche AG; Christine Wurz, Idorsia Pharmaceuticals Ltd.).

For the convenience of users, AGIT publications are available on the Swiss GLP website (see Good Laboratory Practice (GLP)). The Swiss GLP homepage also provides links and references to guidelines, laws and regulations, definitions etc.

AGIT Publications:

- Guidelines for the Validation of Computerised Systems
- Guidelines for the Management of Electronic SOPs in a GLP Environment
- Guidelines for the Archiving of Electronic Raw Data in a GLP Environment
- Guidelines for the Acquisition and Processing of Electronic Raw Data in a GLP Environment
- Guidelines for the Development and Validation of Spreadsheets
- Guidelines for Change Management and Risk Assessment of Validated Computerized Systems in a GLP Environment.
- Position Paper 1: Is it acceptable to destroy the paper originals of raw data and related study documentation, if an image of the paper is captured in an electronic form (e.g. scanned)?
- Guidelines for Collaboration with External IT Service Providers Supporting a GLP Environment