edqm
European Directorate for the Quality of Medicines & HealthCare
Direction européenne de la qualité du médicament & soins de santé

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

General European OMCL Network (GEON) QUALITY MANAGEMENT DOCUMENT

PA/PH/OMCL (08) 69 R7

VALIDATION OF COMPUTERISED SYSTEMS
CORE DOCUMENT

Full document title and reference	Validation of Computerised Systems – Core document PA/PH/OMCL (08) 69 R7
Document type	Guideline
Legislative basis	-
Date of first adoption	May 2009
Date of original entry into force	July 2009
Date of entry into force of revised document	August 2018
Previous titles/other references / last valid version	PA/PH/OMCL (08) 69 3R
Custodian Organisation	The present document was elaborated by the OMCL Network / EDQM of the Council of Europe
Concerned Network	GEON

VALIDATION OF COMPUTERISED SYSTEMS

CORE DOCUMENT

Note: Mandatory requirements in this guideline and its annexes are defined using the terms «shall» or «must». The use of «should» indicates a recommendation. For these parts of the text other appropriately justified approaches are acceptable. The term «can» indicates a possibility or an example with non-binding character.

1. SCOPE

This guideline defines basic principles for the validation of computerised systems used within Official Medicines Control Laboratories (OMCLs) and having impact on the quality of results, document control and data storage [1]. The purpose of this validation is to guarantee confidence in the laboratory data captured, processed, reported or stored by computerised systems. A validated system ensures accurate results and reduces any risks to data integrity.

This document applies to all types of computerised systems used in OMCLs. However, depending on their complexity, the extent of testing and documentation will differ. Computerised systems can be categorised into three types: exempted, simple and complex (see table I in section 3). This document describes a scalable validation approach for simple and complex computerised systems.

2. INTRODUCTION

This guideline outlines general validation principles for computerised systems of OMCLs in accordance with ISO/IEC 17025. It defines general minimum requirements for the validation of different types of computerised systems and additionally gives recommendations for the practical implementation and practical examples specific for OMCLs.

The extent of validation activities should be defined based on risk assessment, considering the dependency of the correctness and traceability of test results of the OMCL on the computerised systems.

Due to the great variety of computerised systems available, it is not possible to state in a single document all the specific validation elements that are applicable.

This guideline is intended for use by OMCLs working under Quality Management Systems based on the ISO/IEC 17025 standard, which use computerised systems for a part or the totality of the processes related to the quality control of medicines.

In order to simplify the guideline, the present core document contains a general introduction and general requirements for different types of computerised systems. This core document is supplemented with system-related annexes containing additional requirements and/or practical examples of validation documentation, which are to be used in combination with the general requirements given here.

This document should be considered as a guide to OMCLs for planning, performing and documenting the validation of their computerised systems. It is left to the professional judgement and background experience of each OMCL to decide on the most relevant procedures to be undertaken in order to give evidence that their computerised systems are working properly and are appropriate for their intended use.

3. DEFINITIONS

Following definitions should be used in order speak the same language in OMCL´s documents. Some of these terms are also used in environments subjected to Good Manufacturing Practice requirements (GMP). It is stressed that GMP requirements do not apply to OMCLs, though for practical reasons the commonly used terms are also used in this document.

Computer system: A system containing one or more computers and associated software.

Computerised system: A broad range of systems including, but not limited to, automated laboratory equipment, laboratory information management, and document management systems. The computerised system consists of the hardware, software, and network components, together with the controlled functions and associated documentation.

Commercial (off-the-shelf, configurable) computerised system: Software defined by a market-driven need, commercially available, and whose fitness for use has been demonstrated by a broad spectrum of commercial users; also known as COTS.

In-house developed (custom-made or bespoke) computerised system: a system produced for a customer, specifically to order, to meet a defined set of user requirements set out in a user requirement specification.

User Requirement Specifications (URS): describes what the system should do. The user requirements contain scientific, business, legal, regulatory, safety, performance and quality aspects of the future system. The user requirements serve as the basis for the Performance Qualification (PQ).

Black Box: a black box in this guideline is a system whose inner working is unknown.

Computerized System validation plan: The validation plan shall be an approved document, which describes the validation activities and responsibilities. The validation plan specifies the Computerized System subjected to validation and compiles the validation activities to be performed and the validation targets/criteria to be fulfilled. The validation plan shall be prepared and approved prior to conducting the test.

DQ (Design Qualification): Documented verification that the proposed design of facilities, systems, and equipment is suitable for the intended purpose

IQ (Installation qualification): Documented verification that a system is installed according to written and pre-approved specifications

OQ (Operational qualification): Documented verification that a system operates according to written and pre-approved specifications throughout specified operating ranges at the customer.

PQ (Performance qualification) or User Acceptance Testing (UAT): Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and pre-approved specifications, within the scope of the business process and operating environment

Black-Box Validation: Validation based on the fact that, for a given computerised system, its source code or design is unknown to the user. Validation is performed from the computerised system or computer system user´s point of view.

Black-Box Test: Periodic check of a computer, computerised system or computerised system based on the black-box validation approach. Black box testing examines the functionality of a system without peering its inner structure or workings.

Table I: Categorisation of computerised systems (based on Reference 6)

	Definition	Examples	Action
Exempted	No calibration function Framework/layered software	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), office application software (Word, Excel), database software (e.g. Oracle, SQL, Access), etc.	None
Simple	Small part of software Restricted customisation	pH meter, oxidisers, incubator, titration processor, colorimeter, thermo hygrograph/hygrometer, balance, particle sizer, UV/VIS spectrometer, liquid scintillation counter, TLC analyser, AAS, micro plate counter, image analyser, polarimeter, CombiStats, etc.	Simplified validation - Calibration - Function control test
Complex	Extended amount of functionality software Extended customisation	LIMS (Laboratory Information Management System), ERP (Enterprise Resource Planning), eDMS (electronic Document Management System), ELN (Electronic Laboratory Notebooks), user-developed Excel spreadsheet, user-developed Access application, 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.	Validation

Remark: Operating systems, office applications, databases and framework packages such as Windows, Excel, Oracle, SAS do not have to be validated by the OMCL. 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) shall be validated.

4. GENERAL REQUIREMENTS FOR COMPUTERISED SYSTEMS

a) *Inventory*

An inventory or equivalent listing of all computerised systems shall be available.

The following minimum information shall be included in the computerised systems inventory:
- identification & version
- purpose
- validation status
- physical or storage (drive and files path) location of the computerised system and related documentation
- responsible or contact person.

For equipment software, this information can be recorded in the equipment logbook.

In the case of local installation (workstation), each individual copy of the software installed on several computers needs its own unique identification (e.g. license).

b) *Validation*

Prior to routine use, the computerised system shall be validated.

The purpose of validation is to confirm that the computerised system specifications conform to the user needs and intended uses by examination and provision of objective evidence and that the particular requirements can be consistently fulfilled.

The extent of validation will depend on the complexity and intended use of the computerised system being validated. The validation effort can be scaled and adapted to the type of system justified by documented risk assessment. The categories mentioned in this guideline (see table I in Section 3) can be used in OMCLs for risk assessment.

URS, validation plans, test and release can also be performed on a rolling basis, if an iterative process (agile software development) is used.

Use of the supplier activities

Validation documents and results of tests performed by the supplier of the software can be incorporated into the OMCL's validation file and does not need to be repeated again by the OMCL. The supplier must be subject to supplier evaluation (e.g. by a questionnaire or an audit).

Validation documents shall verify the computerized system performance, confirming that the system is performing correctly and to standard specifications. Using a supplier´s validation documents, validation in the OMCLs can be reduced to the performance qualification (PQ) phase and ongoing controls indicating the system is working properly.

Validation plan

To ensure the correct implementation of a validation, a plan is needed. The validation plan describes all activities such as review of the URS, review of the development plan (design), test strategy, verification of the data migration (if applicable), review of the validation documents and the acceptance testing of the whole system.

The plan includes the date, the responsible person and the acceptance criteria for each review or test, or at least a reference to these tests.

The validation plan is to be authorised by a responsible person before starting the validation.

The test cases and descriptions can be described later, if an iterative process is used.

Black-Box Validation is an approach to establish by adequate testing that the computerised system meets user needs and intended use, and can involve:

(1) Checking correctness of calculations and formulas and/or analytical results for dedicated samples, references and calibrators;

and/or

(2) Manual calculation of computerised system calculation data (see Annex 1);

and/or

(3) Using a second, independent computerised system tool to review correctness of calculations and/or analytical results;

and/or

(4) Documentation of simulations of invalid or OOS data input and flagging/mistake signals.

For the validation of a computerised system that does not belong to the OMCL (e.g. a computerised system from the Agency/Authority), a simplified validation (e.g.: a Function Control Test) can be performed by the OMCL, taking into consideration the specific functionalities for the OMCL, to check compliance with the ISO 17025 requirements and the OMCL guidelines.

If there is an interface between computerised systems, for example, exchange of information between an analytical system and LIMS, validation of the interface should be considered.

i. Validation of simple systems

Validation of simple computerised systems, e.g. systems with no or limited customisation, will usually rely on instrument calibration and/or a system function test, depending on the type of system.

For analytical instruments where the raw data cannot be modified by the user (e.g. stand-alone balance, pH meter) instrument calibration is considered as sufficient to demonstrate the system is fit for purpose.

For off-the-shelf applications, commercial or supplied by a public agency/authority, a function test shall be performed by the user in order to demonstrate that the application performs properly in the OMCL environment. An example of this approach is given below for CombiStats.

The appropriateness and correctness of the calculations performed by CombiStats is pre- checked and demonstrated by the provider (mainly by the comparison with data published in the book by D.J. Finney [7], a standard reference for statistics in bioassays) so that the computerised system can be considered as fit for purpose (i.e., it fulfils the user requirements). However, an OMCL shall verify that CombiStats works properly in its hardware configuration, once downloaded from the EDQM website. This can be done by comparing the output of the same example reported both in the User Manual (in .pdf format, that will be the "Reference") and in the "example" Directory (in .epa format) automatically downloaded in each user PC Hard Disk. The conclusion regarding the validation status based on this comparison shall be documented.

CombiStats templates and data sheets shall be protected from accidental mistakes and editing. Four different levels of protection are available (each one with or without the use of a password). The User Manual can be used by the OMCL for further details, and to choose the strategy, depending on the internal policy and decision.

ii. Validation of complex systems

Validation of complex computerised systems begins with the definition of the User Requirements Specification (URS), which will serve as a basis for the validation requirements. A validation plan is needed, based on risk assessment, describing the different validation activities planned for the system, and the responsibilities of the different persons involved in the validation process. Then test protocols for IQ, OQ and PQ shall be prepared taking into consideration the user requirements and the acceptance criteria. Test protocols or checklists provided by the supplier can be used for IQ and OQ, when available. The process is finalised after the issuing of the various test reports and a final validation report with the statement that the computerised system is suitable for the intended use. If deviations are identified during validation, they must be addressed and the impact on the adequate functioning of the system shall be evaluated.

In the case of a computerised system for analytical procedures such as an assay, the software is an integrated part of the test procedure. The respective SOP should include or make reference to the sample, the reference standard, reagent preparations, use of apparatus and its computerised system as a unit, generation of calibration curve by means of a computerised system tool, use of calculation formulas, etc.

Examples of validation of complex systems are given for Excel spreadsheets (see Annex 1) and LIMS/ELN/ERP/CDS (see Annex 2).

c) *Logging of issues*

A record of the issues identified by the users and the actions taken should be kept.

d) *Change control*

In the event of changes in the computerised system, including version updates, these should ideally be done first in a test environment after which the validation status needs to be re-established. If a revalidation is needed, it should be conducted not just for validation of the individual change, but also to determine the extent and impact of that change on the entire computerised system.

The extent of the revalidation will depend on assessment of the change(s), which shall be documented. One possible approach could be the use of logbooks as it is done for equipment, and/or using a documented change control procedure.

Automatic system updates should ideally be controlled by IT or a system administrator and installed at pre-defined dates to minimise both disruption and unexpected behaviour of the system. It can be necessary to check the operation of the computerised system following any system updates.

e) *Periodic review*

The OMCL should endorse a policy to check the computerised system periodically, to avoid any error and guarantee the maintained validated status of the system. The frequency of the reviews should be defined on a risk-based approach.

Computerised systems shall be covered by the internal audit strategy.

f) *Security and environmental conditions*

Computerised systems must be protected against any intrusion that could change the data and affect the final results.

Server rooms should have restricted access and have the conditions necessary to ensure the correct functioning of equipment (control of temperature, firefighting measures, Uninterruptible Power Supply - UPS, etc.).

Systems should be accessed only by authorised personnel, using personalised accounts and password or equivalent identification method. The use of shared and generic accounts should be avoided to ensure that actions documented in computerised systems can be attributed to a unique individual. Where personal accounts are not available or feasible, combinations of paper and electronic records should be used to trace actions to the personnel responsible.

Only the responsible person(s) or designated IT personnel should have administrative rights to implement any computerised system updates and/or installations, change critical system settings (e.g. audit trail, time/date) and manage permissions for other users. All routine tasks, such as for analysis, should be based on a user account and password which does not have administrative rights.

Administrative rights should be documented and only be granted to personnel with system maintenance roles (e.g. IT) that are fully independent of the personnel responsible for the content of the records (e.g. laboratory analysts, laboratory management). Where these independent security role assignments are not feasible, other control strategies should be used to reduce data integrity risks.

Computers should be locked after use and the users should not be allowed to change date and time settings.

The hardware used must fulfil the technical requirements so that the work to be completed can be carried out. Such requirements include e.g. minimum system requirements indicated by the manufacturer of the equipment. These requirements should be predefined in accordance with the intended use.

The hardware components must be installed by skilled personnel (e.g. staff from the Information Technology (IT) Unit, a technician from the manufacturer of the equipment, or other trained personnel), and must be checked for their functionality and compared with the requirements.

Computerised systems that are part of test equipment must be labelled unambiguously and records must be kept on relevant hardware configuration, installation and changes. These records can be entered in the logbook/equipment record of the test equipment.

g) *Audit trail*

The computerised system should keep a record of any critical actions that occur, for example who has accessed it and when, any deletion or change of data, etc. If a computerised system does not automatically record an audit trail, an alternative record shall be kept by the OMCL.

Users shall not be allowed to amend or switch off the audit trails or alternative means of providing traceability of user actions.

The need for the implementation of appropriate audit trail functionality should be considered for all new computerised systems. Where an existing computerised system lacks computer-generated audit trails, personnel shall use alternative means such as procedurally controlled use of logbooks, change control, record version control or other combinations of paper and electronic records to meet the requirement for traceability to document the what, who, when and why of an action.

h) *Electronic Signatures*

If electronic signatures are used, a statement about the equivalence of the electronic signature to the handwritten signature or similar legal statement must be available.

i) *Backup*

Traceability must be ensured from raw data to test results. If all or part of the traceability of parameters relevant for the quality of the results is available only in electronic form, a backup process must be implemented to allow for recovery of the system following any failure which compromises its integrity. Backup frequency depends on data criticality, amount of stored data and frequency of data generation.

Based on risk assessment and considering the dependency on computerised systems, the OMCLs should have a policy and procedure in place for ensuring the integrity of backups (secure storage location, adequately separated from the primary storage location, retention time, etc.) – this can be part of a more general 'disaster recovery plan'.

A procedure for regular testing of backup data (restore test), to verify the proper integrity, readability of the electronic record and accuracy of data, should also be in place. This restore test can be integrated into the periodic review of the system.

j) *Archive of superseded computerised system versions*

Superseded versions of software should be archived in a retrievable form if required for access to historical data, according to the OMCL Guideline "Management of Documents and Records". For commercial off-the shelf software, the obligation to archive superseded software versions can be subject to the contract with the provider.

k) *Training*

Correct use and validation of the computerised system shall be ensured. This can be done either by appropriate and documented training or through detailed information in the relevant SOPs or context related information in the software.

Training shall be performed before first use and after every major change in the software (e.g. version upgrade). The persons responsible for the validation shall have training on the validation process.

l) *Documentation*

Table II: Computerised system documentation

Information/documentation that shall be available	**Exempted**	**Simple**	**Complex**
Inventory list, Name, version and unique identification of the computerised system	X	X	X
Original files (CD-ROM…) or storage location to install the computerised system, and computerised system to manage the computer environment		X	X
Date at which the computerised system was put into operation		X	X
Responsible person in charge of the computerised system		X	X
Manufacturer's name, licence number and serial number or other unique identification, where applicable		X	X
Conditions under which the computerised system runs, where applicable (hardware, operating system, …)		X	X
Manufacturer's validation certificate, if available		X	X
Manufacturer's instructions, if available, or reference to their location		X	X
Documentation on validation of configurations/modifications performed by the user that can impact the results			X
Name of the person who developed and validated the computerised system, and the date of validation			X
Source code (if available)			(X)
Operating instruction (SOP)		X	X
Documentation on computerised system periodic review and results of audits			X
Documentation on computerised system validation			X

Information/documentation that shall be available	Exempted	Simple	Complex
Follow-up of failures encountered, maintenance of the process, changes, updated versions and , where appropriate, configuration management		X	X
Training records (depending on the complexity of the system)		(X)	X
Records of the regular testing of backup data (restore test)		X	X

5. REFERENCES AND FURTHER READING

[1] EN ISO/IEC 17025.

[2] Good Practices for Computerized Systems in regulated “GXP” environments. Pharmaceutical Inspection Convention/Pharmaceutical Inspections Co-operation Scheme (PIC/S).

[3] EU Guidelines to Good Manufacturing Practice (GMP). Annex 11. Computerized Systems.

[4] OECD Series on Principles of Good Laboratory Practices and Compliance Monitoring. Number 17. The Application of the Principles of GLP to Computerized Systems. Environment Monograph no. 13 (2016).

[5] U.S. Food and Drug Agency (FDA) General Principles of Computerized system Validation; FDA Glossary of computerized system and computerized system development terminology.

[6] AGIT - Validation of Computerised Systems, V 2.0 (2007).

[7] D. J. Finney - “Statistical Method in Biological Assay”, 3rd Edition, Griffin, London (1978).

[8] WHO TRS 996 Annex 5 - Guidance on good data and record management practices (2016).

6. LIST OF ANNEXES

The latest version applies:

- Annex 1: Validation of Excel Spreadsheets - PA/PH/OMCL (08) 87;
- Annex 2: Validation of complex computerised systems - PA/PH/OMCL (08) 88.