General European OMCL Network (GEON) QUALITY MANAGEMENT DOCUMENT

PA/PH/OMCL (08) 88 R5

VALIDATION OF COMPUTERISED SYSTEMS
ANNEX 2 – VALIDATION OF COMPLEX COMPUTERISED SYSTEMS

Full document title and reference	Validation of Computerised Systems Annex 2 – Validation of Complex Computerised Systems PA/PH/OMCL (08) 88 R5
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	Validation of Computerised Systems Annex 2: Validation of Databases (DB), Laboratory Information Management Systems (LIMS) and Electronic Laboratory Notebooks (ELN) PA/PH/OMCL (08) 88 R
Custodian Organisation	The present document was elaborated by the OMCL Network / EDQM of the Council of Europe
Concerned Network	GEON

**ANNEX 2 OF THE OMCL NETWORK GUIDELINE
"VALIDATION OF COMPUTERISED SYSTEMS"**

VALIDATION OF COMPLEX COMPUTERISED SYSTEMS

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.   INTRODUCTION

This is the 2nd Annex of the core document "Validation of Computerised Systems", and it should be used in combination with the latter when planning, performing and documenting the validation steps of complex computerised systems Excel spreadsheet validation is described in the 1st Annex of the core document and not subjected here.

2.   USER REQUIREMENTS SPECIFICATIONS (URS)

The selection and purchase of new software and the associated computer and laboratory equipment should follow a conscious decision-making process based on the requirements for the intended use of the computerised system. A User Requirements Specification (URS) should describe the functional and technical requirements of the computerised system, as defined by the OMCL, in terms of both software and hardware. It should also cover the aspects of information security and data integrity.

Some of the items that can be included are:

a)   Description of the software used (e.g. Excel, Access, Oracle), including version;
b)   Requirements on hardware components and operating system;
c)   Description of functions;
d)   Description of the attributes of data;
e)   Terminology (e.g. important especially for the consistent description of input masks   / fields);
f)   Database design, including masks and fields as well as a map of the data relationships;
g)   Specifications of macros, formulas and control commands;
h)   Specifications of the data inputs (e.g. format, decimal places, units);
i)   Specification of the mandatory fields for data;
j)   Specifications of the protection of masks, working sheets or the whole application;
k)   Planning of the data migration, if applicable;
l)   Specifications for traceability of data entry and changes (audit trail) of interfaces to other system components, if applicable.

The URS shall be released by a responsible person. Changes to the requirements are possible but the changes should be traceable and the URS document should be version controlled or an equivalent system established in order to ensure traceability. New or changed requirements should be communicated to all persons involved.

3.   INSTALLATION QUALIFICATION (IQ)

The correct installation of the system in the IT environment with defined hardware and operating software shall be documented and tested. Detailed installation procedures should be available and carried out by well-trained personnel only.

Checklists with predefined installation steps and acceptance criteria can ensure the correct installation of the system and the traceable qualification of the installation.

In most cases, the computerised system is connected to a computer network with interfaces to other software (other applications) and hardware (computer equipment or laboratory equipment). It must be ensured that the system is correctly integrated and that all components are operative.

The IQ typically includes:

a) A check of the required system resources both of the server and client, when applicable (e.g. supported operating system, database engine, performance of the processor, free space on the hard disk, memory, access rights for installations);
b) Documentation of the components of the system (as a minimum, a description of the components and version of the relevant components with date of implementation);
c) List of users or user groups with access to the application, including type of access;
d) Integration test and/or communication test for the interfaces to other systems/equipment.

Often the installation is supported by the supplier and the internal IT unit.

4.   OPERATIONAL QUALIFICATION (OQ)

The proper functioning of the software shall be checked by testing the key functions, e.g. calibration and quantification (internal standards, external standards), peak identification, and calculation of system suitability parameters.

Ideally, a raw data set can be used for which the results are known. These raw data sets are often provided by the supplier of the software, are processed by the software and the results are then compared to the expected values.

If no such data sets are available, example raw data sets can be acquired by running typical samples. The results of the processed raw data sets should be verified by recalculating the key parameters (e.g. calibration curves from peak areas of standards) using standard (e.g., spreadsheet) software.

Raw data from the testing of functions affecting the measurement result and its associated measurement uncertainty (input and output data, screenshots) shall be documented within the qualification report.

Operational qualification should be repeated in a risk-based approach after installation of new software modules, new software versions, new service packs, patch updates, or after major changes in the software structure of the computer (e.g. new anti-virus software). A similar approach should be taken for every change in hardware platform or system upgrades.

5.   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 shall be tested in the PQ phase to cover the overall business use of the system in the daily routine.

The PQ typically includes:

a) Tests of functions (e.g. with a data set to ensure each feature of the application is tested);
b) Negative or limit test (e.g. input of values outside the specified range);
c) Test of alarm displays, if applicable (e.g. display of an OOS result);
d) Unauthorised input of data and access to the application;
e) Tests of aberrant data (e.g. input of data in the wrong data format);
f) Backup system and restore test;
g) Verification of data migration, if applicable;
h) Conformity with requirements of data protection, if applicable;
i) Black box test as acceptance testing of the whole system.

Each test scenario should be traceable to the URS being tested and should describe the expected results, the acceptance criteria and the observed results. Each deviation from the expected results and acceptance criteria must be discussed in the test report. A deviation can either lead to a change in the system and the test being run again or be accepted and documented with an update of the corresponding URS. Raw data from the testing (input and output data, screenshots) shall be documented within the qualification report.

6.   RELEASE FOR USE

A summary of all the test findings shall be presented in a validation report, including any deviation and the corrective actions taken. When all deviations are resolved or accepted, a formal release of the system is issued.

7.   ARCHIVING

All documentation related to specification and qualification of complex computerised systems must be retained as long as the application is in use, plus a defined retention period covering all applicable archiving obligations. This obligation can be covered by a contract with the software provider.