



OMCL Network of the Council of Europe QUALITY ASSURANCE DOCUMENT

PA/PH/OMCL (08) 88 R

VALIDATION OF COMPUTERISED SYSTEMS

ANNEX 2: VALIDATION OF DATABASES (DB), LABORATORY INFORMATION MANAGEMENT SYSTEMS (LIMS) AND ELECTRONIC LABORATORY NOTEBOOKS (ELN)

Full document title and reference	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
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	-
Previous titles/other references	-
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 DATABASES (DB), LABORATORY INFORMATION
MANAGEMENT SYSTEMS (LIMS) AND ELECTRONIC
LABORATORY NOTEBOOKS (ELN)**

INTRODUCTION

The present document is the 2nd Annex of the core document “Validation of Computerised Systems”, and it should be used in combination with it when planning, performing and documenting the validation steps of computerised systems.

The core document contains the Introduction, Scope, and general requirements for the validation of different types of computerised systems.

This annex contains additional recommendations, which are to be used in combination with the general recommendations given in the core document.

This document should be considered as a guide to OMCLs for planning, performing and documenting the validation of their computerised systems. It should not be taken as a list of compulsory requirements. 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.

GENERAL APPROACH

Scaleable approach on the extent of the validation

The level of risk affects the extent of the validation. For this case a risk assessment is needed. A risk assessment include the analysis of possible impact of the computerised system on data quality and data integrity.

The level and the extent of the validation is in addition to the risk, depending on the software category.

The computerised system can be mostly considered as follows:

- Infrastructure software, e.g. operating systems or database manager
- Non-configurable software (parts), e.g. firmware-based applications
- Configurable software (parts), e.g. interfaces to apparatus or other software
- Customised software (parts), e.g. Excel with macros, customised dialog windows

Infrastructure software needs to document the software versions and configuration as well as to perform an installation qualification. The validation of a customised software contains a description of the user requirements specification, code review and design review, documentation of the versions and configuration, installation qualification, risk-based tests of the functions and a defined data management.

For this approach it is not necessary to carry out the same activities for the whole system. For each part of the system the validation will be individually described.

Use of the supplier activities

Validation documents and results of tests performed by a supplier of the software, can be transferred to the own validation. These work and tests must be not repeated again by the customer. The supplier should be previously qualified (e.g. by a questionnaire or an audit).

Validation plan

To ensure the correct carry out of a validation, a validation 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, review of the validation documents and the acceptance testing of the whole system.

The plan contains the date, the responsible person and the acceptance criteria for each review or test, at least a reference on 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.

VALIDATION OF DATABASES

Level I. Selection of software and computer equipment

This is the first step in the validation. A user requirements specification (URS) describes the functional, technical and organisational requirements of the system defined by the customer. The realisation and the verification take place according to this URS.

- (1) Description of the used software, including version (e.g. Excel, Access, Oracle)
- (2) Requirements on hardware components and operating system
- (3) Description of functions
- (4) Description of the attributes of data
- (5) Terminology (e.g. importantly for the consistent inscription of input masks / fields)
- (6) Database design, including masks and fields as well as a map of data relationship
- (7) Specifications of macros, formulas and control commands
- (8) Specifications of the data inputs (e.g. format, decimal places, units)
- (9) Specification of the mandatory fields for data
- (10) Specifications of the protection of masks, working sheets or the whole application
- (11) Planning of the data migration, if applicable
- (12) Specifications of interfaces to other system components, if applicable

In case of a simple database, a sketch of the data flow as database design is sufficient. The specifications (URS) should be released by a responsible person. Changes on the requirements are possible. The changes should be traceable and the URS receives a new version number. New or changed requirements should be communicated to all involved persons.

Level II. Installation and release for use

The correct installation of the system in the IT environment with defined hardware and operating software is documented and tested. In most cases, the DB, LIMS or ELN is embedded in a computer network system with interfaces to other software's and hardware's. The correct integration of the system as well as that all components are operative must be ensured.

Installation

- (1) Check of the required system resources (e.g. performance of the processor, free space on the hard disk, access for installations)
- (2) Documentation of the components of the system (at least description of the component and version of the relevant components with date of implementation)
- (3) List of users or user groups with access to the application, including type of access
- (4) Integration test and/or communication test (e.g. store a set of known data in the database and process the data, if a calculation or another process is programmed, restore and print the data and compare with the acceptance criteria)

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

Release for use

- (1) Design review
- (2) Tests of functions (e.g. with a set of data each feature of the database is tested)
- (3) Negative or limit test (e.g. input of values outside the specified range)
- (4) Test of alarm displays, if applicable (e.g. display of a OOS result)
- (5) Unauthorised input of data and access to the application
- (6) Tests of misentry (e.g. input of data in the wrong data format)
- (7) Back up system and restore test
- (8) Verification of the data migration, if applicable
- (9) Conformity with requirements of the data protection, if applicable
- (10) Black box test as acceptance testing of the whole system

On this part the compliance with the URS is to be checked.

The number of data sets used for the functionality test depends on the evaluated risk class. At least two values within the normal range should be applied.

As limit test or negative test, at least one value below and one value above a limit should be used. The same test strategy can be used for the check of an alert function.

In case of a database with many functions, a reduced test size on the key functionalities is possible. This is a risk-based decision and should be traceable documented. It is also possible to perform black box tests of the most important use cases of the database instead of tests of the individual functions.

To show the robustness of the database, unauthorised and incorrect inputs of data are performed.

The verification of the data migration goes from six data records up to 100 % of the migrated data. The random sample depends on the evaluated risk class. The data in the target system are compared with the data in the source system. For such kinds of verifications automated tools are available.

Level III. Periodic and motivated software functionality checks

Periodic checks (black box test), especially after major changes and in regular intervals, are performed to ensure the proper work of the whole system during the life time.

Documentation

Additional to the list of software documentation according to the core document of the validation of computerised systems some special aspects are to be into account.

- (1) System description of the database (e.g. system diagram, programme process, relationships of cells and tables, macros, formulas)
- (2) Screenshots of the relevant working sheets and masks
- (3) User requirements specification, at least the last relevant version of the URS
- (4) Reports of the installation qualification, including the configuration
- (5) Test descriptions, records and results of the verification
- (6) Validation report, if applicable
- (7) Uniquely identification of the version of the database
- (8) Training plans and records, if applicable
- (9) User documentation, if applicable
- (10) Maintenance documentation, if applicable

The documentation should allow the traceability of the validation as well as the maintenance and the development of the database at any time of the life cycle by a third party. Every change in documents should be traceable.

Management

This part is not a typical step of a validation process, but it contains information's which are relevant for the specification and validation of the system.

A database is valid during the time of use, if the maintenance of the database is guaranteed.

- (1) Configuration management (at each time the configuration of the computerised system, which contains the database, should be traceable, including date of the integration of new components or versions)
- (2) Change control (every changes in the design of the database should be traceable and for major changes a previous release by a responsible person is needed)
- (3) Management of patches and updates on the operating system (at least documentation of the performed patches and updates, rules of patches/updates e.g. over the night or week end, a black box test after the installation of the patch/update if needed)
- (4) Insistent and interruption management (collection of the deviations an failures in a list, e.g. corrective action and preventive action / CAPA)
- (5) Help desk organisation, if applicable
- (6) Safety copy of the application
- (7) Data security (login, password, access rules)
- (8) Backup strategy (e.g. medium, incremental or complete backup, time period)
- (9) Disaster recovery concept, if applicable
- (10) Training concept, if applicable

In case of a simple database, the requirements on the database management are reduced. The list above is especially valid for complex databases.

The responsibilities for the configuration management between the intern IT unit and the OMCL should be described. This is also important for the patch and update management as well as for backups.

VALIDATION OF LIMS / ELN

In the background of a LIMS or an ELN a database is running. All requirements, which are listed in chapter “Validation of databases”, are also valid for LIMS or ELN. The aspects, which are marked as “if applicable” in the previous chapter, are particularly relevant for LIMS.

Special notes and additional requirements are described in the following topics.

Level I. Selection of software and computer equipment

The user requirements specification should contain all relevant functional, technical and organisational specifications. It should cover also the aspects of information security and data protection.

Each requirement should be described in one line of the URS. Each line should be assigned with a unique number. This number helps to refer the requirement in the development process as well as in the validation process.

Level II. Installation and release for use

Detailed installation procedures should be available. The installation should be carried out only by well trained personnel.

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

It is important to take the following aspects into account of the validation process:

- (1) IT network (check of the required system specification and performance data)
- (2) Clients (the configuration of the clients should be known)
- (3) LIMS or ELN server (see under IT network)
- (4) Periphery components and interfaces (the function of each component and interface should be checked)
- (5) Source code of the software (source code, coding rules and coding tools should be known and the access to them should be guaranteed)
- (6) Data (the data integrity should be showed by comparison of the original data with reprocessed data as well as the use of restricted access and an audit trail)
- (7) Manuals and procedures (all relevant documents such as installation procedure, software description, validation procedures, training and user manuals, maintenance manual, backup and restore procedure, procedure for change management and a development documentation should be available)
- (8) Supplier (the supplier should be qualified)
- (9) Personnel (the personnel should be trained and qualified, a training strategy and a training plan of the end users should be available)

Level III. Periodic and motivated software functionality checks

Periodic checks (black box test) of the main functions, each with one test case.

VALIDATION OF EXISTING SOFTWARE

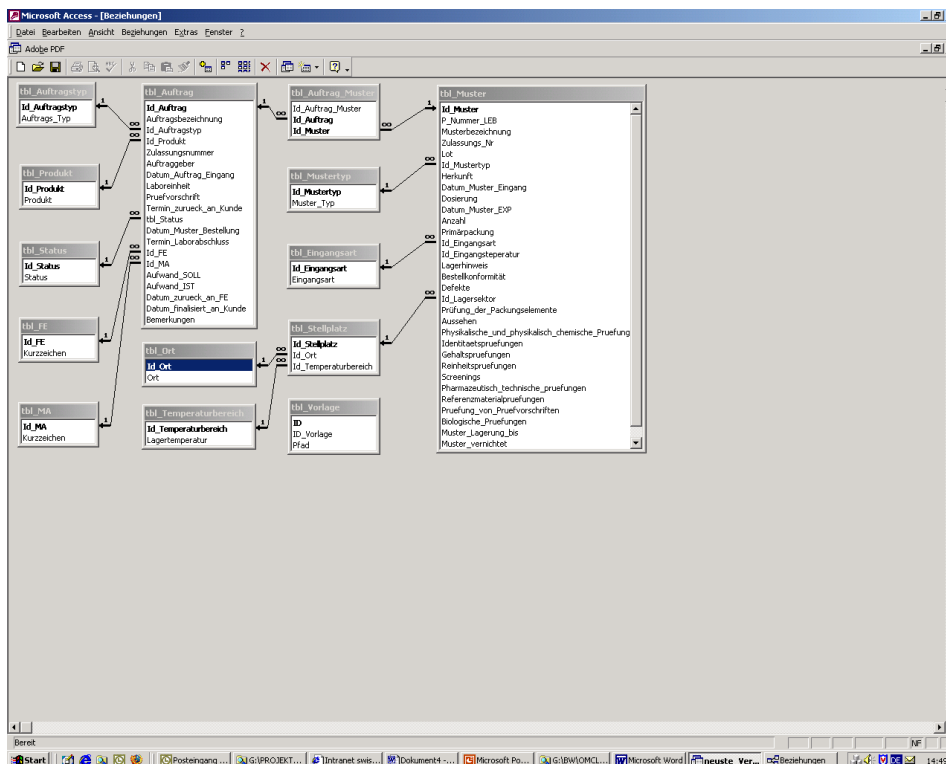
The previous requirements are applicable for new databases and LIMS/ELN.

For the retrospective validation of existing software, in particular the following points are to be considered.

- (1) Perform a risk assessment
- (2) Inventory of all existing documents (e.g. system descriptions, concepts)
- (3) Verification of correct installation (e.g. requirements on the operating system)
- (4) Create an experience report (summary of the experience with the software: How long is the software running? Failures?)
- (5) Addition of missing documents (at least functional description as an overview or basic specifications)
- (6) Overall test (typical application with a comparison of the result with the expected value)
- (7) Formal release for use

EXAMPLES

Map of data relationship (access database)

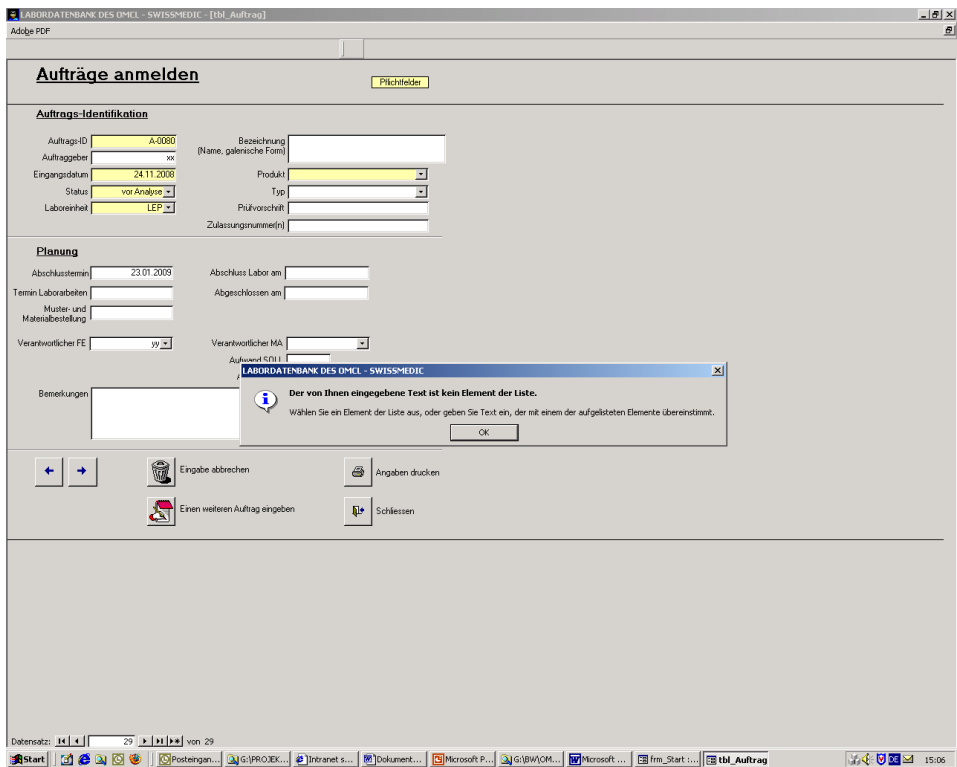


This map can be used in the specification step of a database (database structure) as well as for the design review and as documentation of this verification.

Screenshot of an input mask with mandatory fields

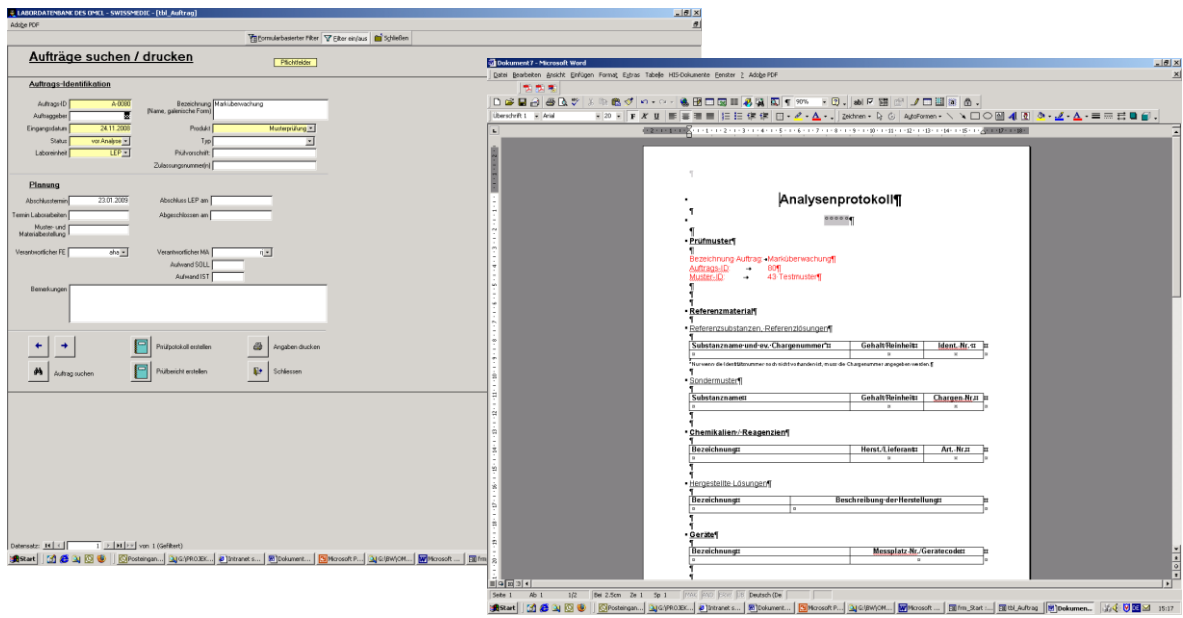
This screenshot can be used as documentation of relevant forms with the specification of mandatory fields as well as for the verification of these fields.

Screenshot of an unauthorised access or a misentry with an error message



This screenshot can be used as documentation of the verification of intentional unauthorised access or a misentry.

Screenshots of a comparison of entered data with data output



These screenshots can be used as documentation of an integration or communication test.

Validation of a simple database

For example a database is only use for generating pre-filled reports (header and footer, data as product name, batch number or sample ID). The results will be filled in by hand, without calculations.

Test:

A report is printed and compared with the known data (sample ID etc). This comparison is performed once. Other activities are not necessary.

Tests against the specifications

Functional specification (part of the URS):

ID	description
100.1	Enter of a pH value and comparison with the specification. Viewing an out of specification in red.

pH specification of product XY: pH 6.0 to 8.0

Tests:

1. Enter pH 7.2 → correct value, within spec
2. Enter pH 6.1 → correct value, within spec
3. Enter pH 5.9 → correct value, out of spec → result in red
4. Enter pH 15.2 → false value → error message

Explanation:

The comparison with the specification is critical. Risk: false assessment of the sample as a result of an incorrect comparison with the specification.

REFERENCES

(If the document version is not indicated, the latest version applies)

- 1) OMCL guideline on Validation of computerised systems – Core document (PA/PH/OMCL (08) 69)
- 2) Good Automated Manufacturing Practice (GAMP 5)
- 3) ISO / IEC 17025:2005 General requirements for the competence of testing and calibration laboratories
- 4) Guidance for the management of computers and software in laboratories with reference to ISO/IEC 17025:2005 (Technical Report No. 2/2006 October 2006, eurolab)