



OMCL Network of the Council of Europe QUALITY ASSURANCE DOCUMENT

PA/PH/OMCL (08) 69 3R

VALIDATION OF COMPUTERISED SYSTEMS

CORE DOCUMENT

Full document title and reference	Validation of Computerised Systems - Core Document PA/PH/OMCL (08) 69 3R
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

VALIDATION OF COMPUTERISED SYSTEMS

CORE DOCUMENT

SCOPE

This guideline defines basic principles for the validation of computerised systems used within Official Medicines Control Laboratories (OMCLs) with impact on quality of results. The purpose of this validation is to guarantee the confidence in scientific results obtained with each computerised system. A validated system ensures accurate results and reduces the risk of failure of the system.

This document covers in-house and commercial software for calculation, database computerised systems, Laboratory Information Management Systems (LIMS), Electronic Laboratory Notebooks (ELN) and computers as part of test equipment.

INTRODUCTION

This guideline outlines general validation principles for computerised systems of OMCLs in accordance with ISO/IEC 17025. It gives general requirements and it also lists the minimum elements required for the validation of different types of software. Actually, due to the great variety of software, it is not possible to state in one 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, and it is not addressed to manufacturers working under GMP requirements.

In order to simplify the management of the guideline, the present document contains only a general introduction and general requirements for different types of computerised systems. The 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 recommendations given in the core document.

The list of annexes, included in this document, will be updated as soon as new annexes are issued.

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.

DEFINITIONS

Computer system: Computer hardware components assembled to perform in conjunction with a set of software programmes, which are collectively designed to perform a specific function or group of functions.

Computerised system: a computer system plus the controlled function that it operates. Includes hardware, software, peripheral devices, personnel, and documentation; e.g., manuals and Standard Operating Procedures (SOPs).

Commercial (off-the-shelf, configurable) software: Configurable programmes that can be configured to specific user applications by “filling in the blanks”, without altering the basic programme.

In-house developed software: system developed by the user (or by a contracted company), with the purpose of specifically meeting a defined set of user requirements.

Electronic laboratory notebook (ELN): software programme designed to replace paper laboratory notebooks.

Laboratory Information Management System (LIMS): Automated laboratory systems that collect and manage data.

1. HARDWARE

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

Computerised systems that are part of test equipment must be labelled unambiguously.

For computerised systems which are components of test equipment, records must be kept on hardware configuration, installation and changes. These records can be entered in the logbook of the test equipment.

2. GENERAL REQUIREMENTS FOR SOFTWARE

Inventory

An inventory or listing of all computerised systems should be available.

The following minimum information should be included in the computerised systems inventory:

- unique identification
- purpose
- validation status
- physical or storage (drive and files path) location of the software and related documentation
- responsible or contact person

In the case of local installation (workstation), each copy of the software needs its own unique identification.

In the case of software related to scientific equipment (e.g. HPLC) its identification (such as licence number or serial number, and version number) should be independent from the equipment identification, whenever possible.

Validation of the software

Prior to routine use, the software should be validated.

Validation consists in confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.

Change control

In case of changes in the software, the validation status needs to be re-established. If a revalidation analysis 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.

In the same way, changes in the computer environment could have an impact on the software running. In this case, a revalidation could be required.

In both cases, the extent of the revalidation will depend on the nature of the change. The nature of the changes should be documented.

Automatic updates should ideally be controlled by IT or a system administrator and installed at pre-defined dates to minimize both disruption and unexpected behaviour of the system. Following installation of updates, verification should be carried out, the extent of which will depend on the extent of the update(s). Each update should be documented.

Note: this does not necessarily apply to service patches for commercial office software.

Verification of the software

Commercial software should be checked at installation.

Concerning in-house software, it should be verified not only at installation but also on a regular basis to avoid any error and guarantee good results. The regularity of the verification depends on software safety, usage frequency and the possible impact, if there is a failure.

In both cases, the OMCL's policy should be described in a procedure.

Protection of the software

Software must be protected against any intrusion that could generate wrong scientific results. One way could be to secure software or computers/systems access by a password. It must also be protected against any external interference that could change the data and affect the final results.

Backup

Traceability must be ensured from raw data to 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. Back up frequency depends on data criticality, amount of stored data and frequency of data generation.

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, etc) – this may be part of a more general 'disaster recovery plan'.

A procedure for regular testing of backup data (restore test), to verify the proper integrity and accuracy of data, should be also in place.

Archive of superseded software versions

Superseded versions of software should be archived (if required for access to historical data) for at least 5 years¹ in a retrievable and readable electronic format.

Note: this requirement is not applicable to commercial off-the-shelf office software (including service patches), software that is archived by a qualified subcontractor or when historical data (raw data and results) are documented in paper format

Identification of software version

The version and name of the software should be displayed to the user at an appropriate stage of the operation of the software (e.g. on the screen when opening the application) and it should be traceable in any reports generated by the software.

For laboratory software on computers as part of test equipment, software updates including the version number should be traceable in the equipments' log book.

Review of computerised systems

Risk management activities and/or audits should be performed on a regular basis for computerised systems.

Training of software operators

Correct operation of the software should be ensured. This may be done either by appropriate and documented training or through detailed information in the relevant SOPs.

3. VALIDATION OF CALCULATION SOFTWARE

Commercial or in-house developed software may be used for calculation and data analysis.

The requested documentation/information, applicable to both commercial and for in-house developed software for calculations, is shown in Table I.

a) Commercial software

If several pieces of commercial software are available, the laboratory should select the one that better fits the intended purpose.

According to ISO/IEC 17025 standard², commercial off-the-shelf software (e.g. word-processing, database and statistical programmes), in general use within their designed application range, may be considered to be sufficiently validated. However, laboratory software configurations/modifications should be validated.

¹ OMCL Guideline "ARCHIVING WITHIN THE OMCL NETWORK"

² ISO/IEC 17025 standard, chapter 5.4.7 and 5.5.5.

A reduced validation procedure (of these configurations/modifications) is acceptable if the documentation supplied with the commercial off-the-shelf product has been reviewed and considered as fulfilling the user requirements.

b) In-house software

If in-house software are used, they are under the supervision of the main user; they must be validated, checked and secured. For more details on validation, see Annex 1.

General requirements:

- Concerning spreadsheets (e.g. Excel[®]), for security reasons, all cells including calculations must be locked in such a way that formulas are not accidentally overwritten. Free access should only be given to cells to be filled in with data. Formulas should also be protected from accidental input of inappropriate data type (e.g. text in a numeric field).
- Each calculation algorithm should be tested with another validated software (the software version used for the calculations should be traceable in the records) or by a pocket calculator and documented or in comparison with published data.
- A known dataset should be used for the verification of the software, for which the expected final results are identified.

Table I: Software documentation

Information/documentation that should be available	Commercial	In-house
Name, version and unique identification of the software	X	X
Original files (CD-ROM...) or storage location to install the software and software to manage the computer environment	X	X
Date at which the software was put into operation	X	X
Current physical location, where appropriate	X	X
Responsible person in charge of the software	X	X
Manufacturer's name, licence number and serial number or other unique identification	X	
Conditions under which the software runs, where applicable (hardware, operating system,...)	X	X
Manufacturer's certificate of validation, if available	X	
Manufacturer's instructions, if available, or reference to their location	X	
Documentation on validation of configurations/modifications performed by the user that may impact the results (see Annexes)	X	
Name of the person who developed and validated the software, and the date of validation		X
Source code, if available		X
Operating rules, where appropriate		X
Documentation on software regular verification		X
Documentation on software validation (see Annexes)		X
Follow-up of encountered failures, maintenance of the process, updated versions and , where appropriate, configuration management	X	X

4. VALIDATION OF DATABASE COMPUTERISED SYSTEMS

Databases used for the storage and retrieval of test results and preparation of test reports, which have been developed in-house by using commercial software (e.g. Access[®]), in its normal configuration, are considered to be sufficiently validated.

Nevertheless, the following minimum documentation/information has to be kept up to date, in the corresponding file of each database:

- A schematic representation of the database.
- Changes to forms, queries, macros, field types or properties that could have an impact on the quality of results should be traceable.
- Each user should have a personal access code.
- User rights should be defined.
- Operating rules should be recorded.
- Any modification for improvement or failure should be documented.

5. VALIDATION OF LIMS and ELN

For commercial Laboratory Information Management System (LIMS) and Electronic Laboratory Notebook (ELN), system validation must ensure that the entire system has been properly tested. For more details on validation, see Annex 2.

Validation of any modification, configuration or calculation that may have an impact on the results are under the users' responsibility (see chapter 3.a and table 1 for commercial software).

6. VALIDATION OF COMPUTERS AS PART OF TEST EQUIPMENT

In some test methods (e.g. HPLC, particle counting), test equipment is used, which is controlled by computerised systems. In doing so, the raw data are in general also evaluated directly via the computer. The quality of such test results is thus largely dependent on the correct use of the software and the functionality of the computerised system. For more details on validation, see Annex 3.

As part of the equipment qualification, the computerised system, together with the software relating to it must be validated with regard to reliability, accuracy, and reproducibility (it may however be sufficient to qualify the testing equipment with the software as a whole).

A revalidation is required if modifications to the computerised systems (hardware or software) might influence the quality of the test results.

REFERENCES

For all references, the latest version applies.

- 1) Good Automated Manufacturing Practices (GAMP).
- 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 10. The Application of the Principles of GLP to Computerized Systems. Environment Monograph no. 116.
- 5) U.S. Food and Drug Agency (FDA) General Principles of Software Validation; FDA Glossary of computerized system and software development terminology (http://www.fda.gov/ora/inspect_ref/igs/gloss.html).

LIST OF ANNEXES (the latest version applies):

- Annex 1: Validation of computerised calculation systems - PA/PH/OMCL (08) 87
- Annex 2: Validation of databases, Laboratory Information Management Systems (LIMS) and Electronic Laboratory Notebooks (ELN) - PA/PH/OMCL (08) 88
- Annex 3: Validation of computers as part of test equipment - PA/PH/OMCL (08) 89



OMCL Network of the Council of Europe QUALITY ASSURANCE DOCUMENT

PA/PH/OMCL (08) 87 2R

VALIDATION OF COMPUTERISED SYSTEMS

ANNEX 1: VALIDATION OF COMPUTERISED CALCULATION SYSTEMS: EXAMPLE OF VALIDATION OF IN-HOUSE SOFTWARE

Full document title and reference	Validation of Computerised Systems Annex 1: Validation of computerised calculation systems: example of validation of in-house software PA/PH/OMCL (08) 87 2R
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 1 OF THE OMCL NETWORK GUIDELINE
“VALIDATION OF COMPUTERISED SYSTEMS”**

VALIDATION OF COMPUTERISED CALCULATION SYSTEMS

EXAMPLE OF VALIDATION OF IN-HOUSE SOFTWARE

INTRODUCTION

The present document is the 1st 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 process of computerised systems.

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

This Annex presents an example of Excel[®] spreadsheet validation, which is 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.

1. SOFTWARE PRESENTATION AND GENERAL INFORMATION

This software's aim is to calculate a vaccine titration (Figure 1). From results obtained for a reference product (height measured at 4 concentrations), a calibration curve and its formula are provided. Both of them are needed to calculate the concentrations corresponding to the height measured for the tested vaccine.

In Figure 1, grey cells are filled with numerical data from experimentation and are the only ones that can be changed by the operator. All cells including formula are locked. No more than one cell from the calibration range can be empty; all cells for vaccines must be filled to guarantee proper use.

To access the software, a password is needed to log on the computer.

Back ups are regularly performed to ensure original files preserving.

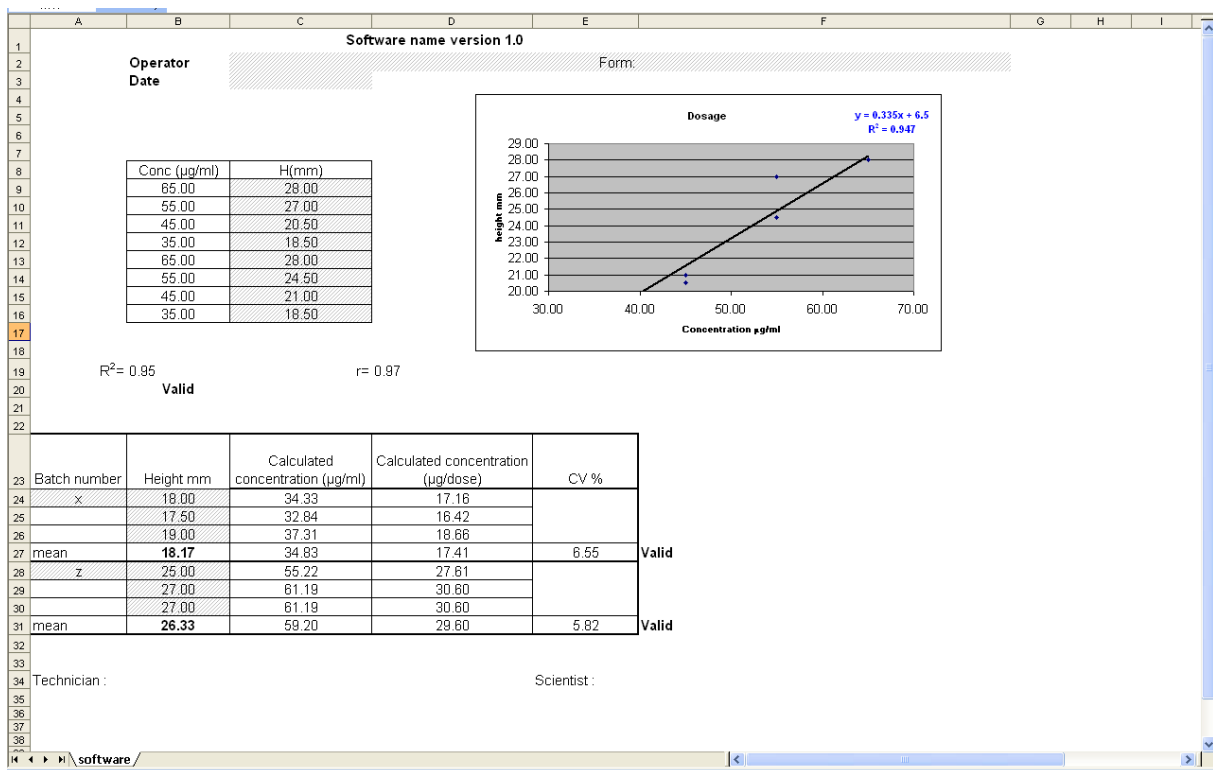


Figure 1. Software presentation

2. VALIDATION STAGES

The different stages of the validation are:

- 2.1 Printing of formulas
- 2.2 Validation of the calculations
- 2.3 Validation certificate
- 2.4 Software installation and documentation

2.1 Printing of formulas

In order to validate the Excel[®] spreadsheet, formulas are printed, and the print is kept in the software validation file (Figures 2.1 and 2.2).

A		B		C		
1				Software name version 1.0		
2						
3	Operator					
4	Date					
5						
6						
7						
8						
9		Conc (µg/ml)		H(mm)		
10		65				
11		55				
12		45				
13		35				
14		65				
15		55				
16		45				
17		35				
18						
19		R ² =COEFFICIENT.DETERMINATION(\$C\$9:\$C\$16,\$B\$9:\$B\$16)				r ²
20		=SI(B19<0.85;"Not Valid";"Valid")				
21						
22						
23	Batch number	Height mm		Calculated concentration (µg/ml)		
24	x	18		=(B24-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
25		17.5		=(B25-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
26		19		=(B26-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
27	mean	=(B24+B25+B26)/3		=(B27-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
28		z	25	=(B28-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
29			27	=(B29-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
30			27	=(B30-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
31	mean	=(B28+B29+B30)/3		=(B31-ORDONNEE.ORIGINE(\$C\$9:\$C\$16,\$B\$9:\$B\$16))/PEUTE(\$C\$9:\$C\$16,\$B\$9:\$B\$16)		
32						
33						
34	Technician :					
30/04/2009		Software name version 1.0				

Figure 2.1. Printed formulas of the software

D		E		F	
1				Form :	
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19		=COEFFICIENT.CORRELATION(\$C\$9:\$C\$16,\$B\$9:\$B\$16)			
20					
21					
22					
23		Calculated concentration (µg/dose)		CV %	
24		=SI(C24<0;"ERREUR";C24/2)			
25		=SI(C25<0;"ERREUR";C25/2)			
26		=SI(C26<0;"ERREUR";C26/2)			
27				=(ECARTYPE(C24:C26)/C27)*100	
28		=SI(OU(\$B\$20="Invalid experiment";E27>10);"Not Valid";"Valid")			
29		=SI(C28<0;"ERREUR";C28/2)			
30		=SI(C29<0;"ERREUR";C29/2)			
31				=(ECARTYPE(C28:C30)/C31)*100	
32		=SI(OU(\$B\$20="Invalid experiment";E31>10);"Not Valid";"Valid")			
33		Scientist :			
34					
30/04/2009		Software name version 1.0			

Figure 2.2. Printed formulas of the software (Cont.)

2.2 Validation of the calculations

All calculations are verified with a system completely independent from the self developed software. One part of the recalculation is performed by validation versus a commercial software, the other part with a pocket calculator.

2.2.1 Validation of the calculations versus commercial software

Then, a dataset as close to real values as possible is chosen (Figure 1). Excel[®] calculations are compared to the results given by commercial software, since it is considered as validated (Figure 3). The commercial software provides the coefficient of correlation, R^2 and the coefficients of the calibration curve. As no discrepancy occurs, the validation of this part of calculation is considered as fulfilled.

```

Regression Analysis - Linear model: Y = a + b*X
-----
Dependent variable: H
Independent variable: Conc
-----

```

Parameter	Estimate	Standard Error	T Statistic	P-Value
Intercept	6.5	1.6569	3.92299	0.0078
Slope	0.335	0.0323393	10.3589	0.0000

```

-----
Analysis of Variance
-----

```

Source	Sum of Squares	Df	Mean Square	F-Ratio	P-Value
Model	112.225	1	112.225	107.31	0.0000
Residual	6.275	6	1.04583		
Total (Corr.)	118.5	7			

```

-----
Correlation Coefficient = 0.973163
R-squared = 94.7046 percent
Standard Error of Est. = 1.02266

The StatAdvisor
-----
The output shows the results of fitting a linear model to describe
the relationship between H and Conc. The equation of the fitted model
is

H = 6.5 + 0.335*Conc

Since the P-value in the ANOVA table is less than 0.01, there is a
statistically significant relationship between H and Conc at the 99%
confidence level.

The R-Squared statistic indicates that the model as fitted explains
94.7046% of the variability in H. The correlation coefficient equals
0.973163, indicating a relatively strong relationship between the
variables. The standard error of the estimate shows the standard
deviation of the residuals to be 1.02266. This value can be used to
construct prediction limits for new observations by selecting the
Forecasts option from the text menu.

```

Figure 3. Commercial software results

2.2.2 Validation of the calculations with a pocket calculator (Manual calculations)

Concerning the other calculations, from printed formula from the spreadsheet, concentrations are calculated using a pocket calculator (Figure 4) and then compared to the results of Figure 1. As no discrepancy occurs, the validation of this part of calculation is considered as fulfilled.

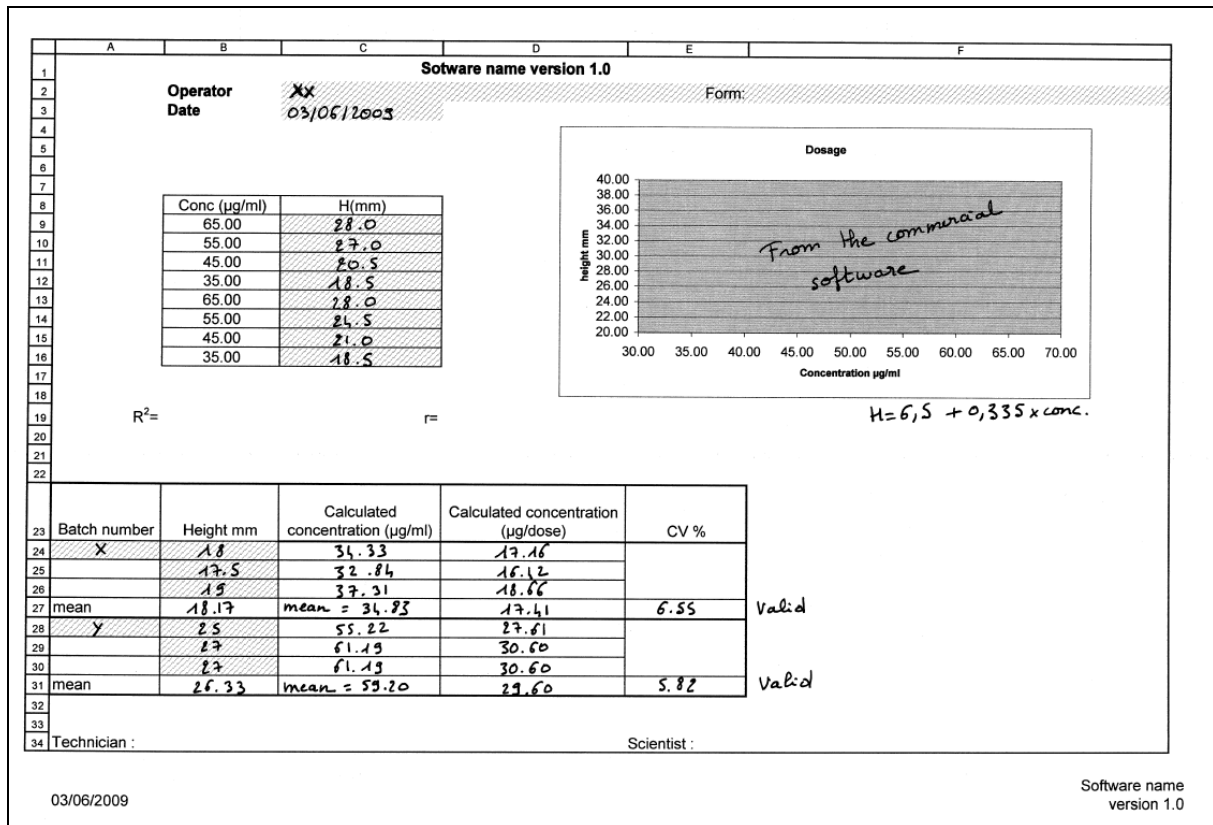


Figure 4. Manual validation

Moreover, calculations in paragraph 2.2.1 and 2.2.2 are re-performed with other datasets including exceptional situations, as for example: OOS-results, missing data, or nonsense-data. Calculations are also validated under these conditions (data not shown).

At this stage, the software is considered as validated.
 To ensure traceability of validation a certificate is emitted.

2.3 Validation certificate

As the software is validated, a certificate of validation is provided. It includes the name and the version of the software, the date of validation, the person responsible for the validation, the person responsible for the release for use of the software and their signatures. This document (Figure 5) is kept in the software documentation.

Name of the control laboratory

Certificate of software validation

Name of the software:
Validated version:
Date of validation:
Person responsible for the validation:
Person responsible for the release for use of the software:
Conclusion of validation:

Date and signature of person responsible for the validation

Date and signature of person responsible for the release for use of the software

Figure 5. Certificate of software validation

Comment: This certificate is an example of the formalisation of the validation. Alternatively, a Quality Assurance form could be used.

Moreover, the person responsible for the validation can be the same as the one responsible for the release for use of the software.

2.4 Software installation and documentation

The concrete installation is completed after validation of the software. The operator signs the life form to attest its proper installation. This form, which actually is a QA document, includes the name of the software, unique identification, localisation, and person responsible for the software. It includes also verification and other specification as updates or any problem encountered (Figure 6). Verification is completed after installation and reported in the life form.

Life Form		Name of the software		Form number	
Unique identification:		Manufacturer:		Localization:	
		Person responsible for the software:			

Date	Encountered problem	Intervention	Comment Next intervention	Operator	Signature of the person responsible for the software
30/04/2009		Installation		XC	×
30/04/2009		Verification	Next verification 30/10/2009	XC	×

AQ number : ELYO/XXX Version Y 30/01/2007
 Validated by ZZZ QA Manager registration

Figure 6. Life Form

Comment:

Another way to secure this Excel spreadsheet would have been to install the software on a network-drive with restricted access. Only authorised staff would be able to write on this drive. The user would have no right to save data or spreadsheets and would have only the right to fill the (permitted) cells and to print the data.

3. REGULAR VERIFICATION OF THE SOFTWARE

Regularly (for example, every 6 months) or after every change performed in the soft- or hardware configuration, the software is checked to be sure that results have not changed. A known dataset is used and the results are compared to the standard one (Figure 1).

In order to help the operator, verification instructions with required information have been written (Figure 7).

Results from the verification are printed, dated, signed and kept with the life form.

Each verification is registered in the life form (Figure 6) with the following information: Date of operation, intervention (i.e. verification), comments, and operator's signature.

Comments:

In case of an installation on a network drive with restricted access (cf. comment in chapter 2.5), the regular verification would be optional.

The check could have included the verification if the save date of the software is still the same as after original installation.

Verification instructions

This document provides instructions for the periodic review of the software described below.

Localisation of the original file: C:\Name of the software\name.xls

Verification: All grey cells must be completed and compared to the template below.

- **Information:** Name of the operator, form number and date of verification.
- **Reference product data:** Heights.
- **Vaccine data:** Batch number and heights for the two batches.

Results: Print, date, sign and keep the results in the software file.

Life form: Register your verification in the software life form.

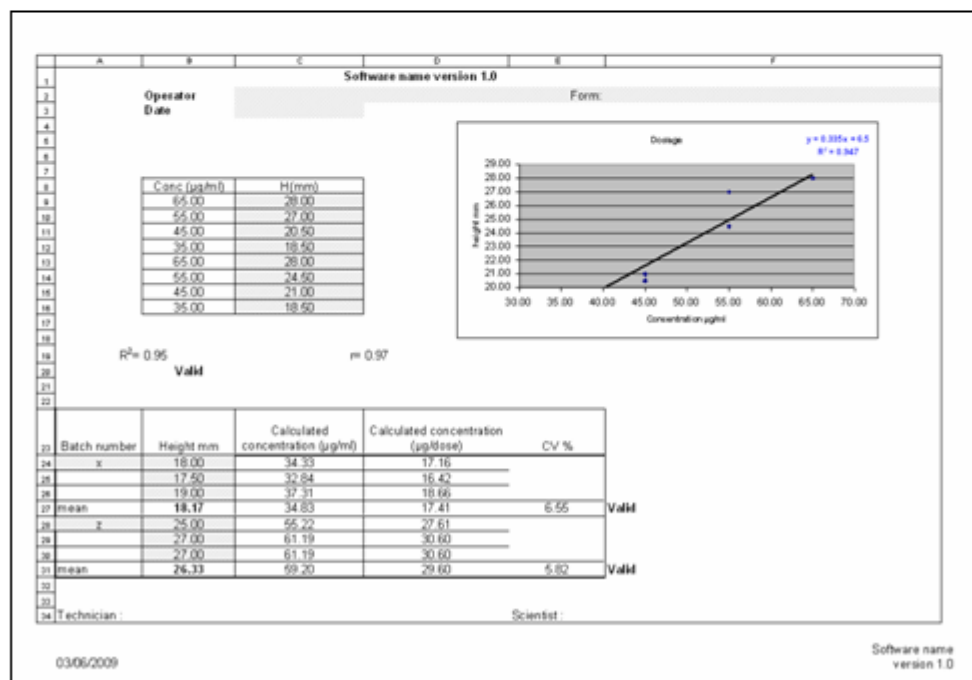


Figure 7. Verification instructions

4. SPECIFIC DOCUMENTATION

According to the guideline, in-house software should be completed with the following specific documentation. The correspondence between the guideline table and each information/documentation of the validation of this Excel® software (Specific documents and Figures) is indicated below:

Information/documentation that should be available	In-house	Specific documents	Figures
Name, version and unique identification of the software	X	Life form and printings	Figure 6
Original files (CD-ROM...) or storage location to install the software and software to manage the computer environment	X	Backup of the software on the network	
Date at which the software was put into operation	X	Life form	Figure 6
Current physical location, where appropriate	X	Life form	Figure 6
Responsible person in charge of the software	X	Life form	Figure 6
Conditions under which the software runs, where applicable (hardware, operating system,...)	X	Not applicable	
Name of the person who developed and validated the software, and the date of validation	X	Validation certificate	Figure 5
Source code (if available)	X	Printing of formulas	Figures 2.1 and 2.2
Operating rules, where appropriate	X	Not appropriate	
Documentation on software regular verification	X	Life form Verification instructions	Figures 6 and 7
Documentation on software validation	X	Software validation file	Figures 1, 2.1, 2.2, 3, 4 and 5
Follow-up of encountered failures, maintenance of the process, updated versions and, where appropriate, configuration management	X	Life form	Figure 6



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

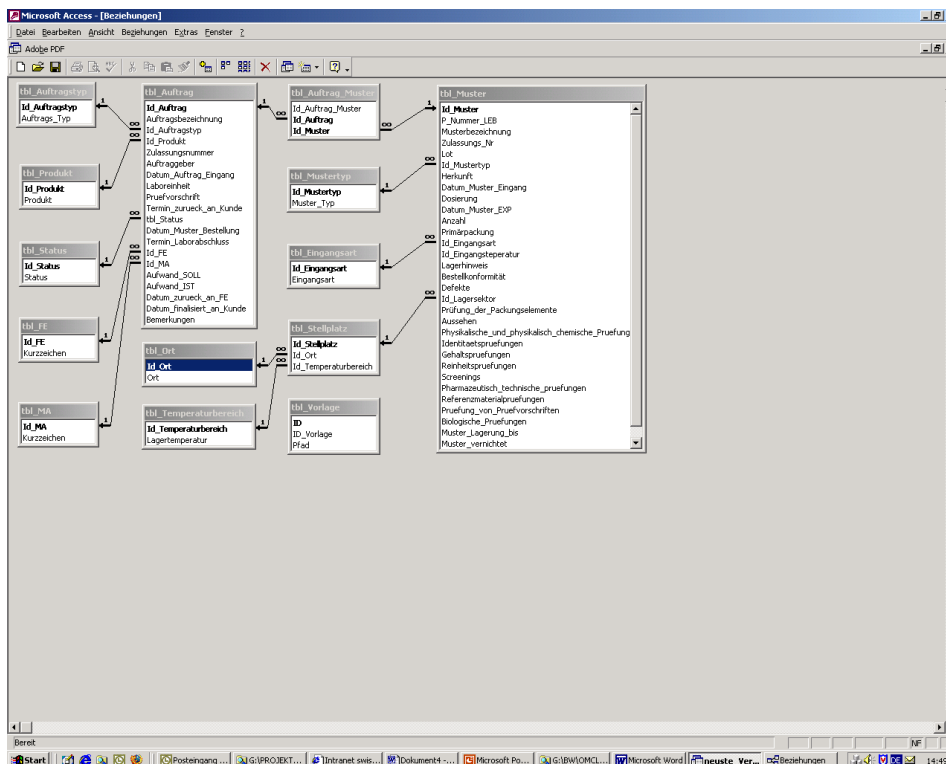
The previous requirements are applicable for new databases and LIMS/ELN.

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)

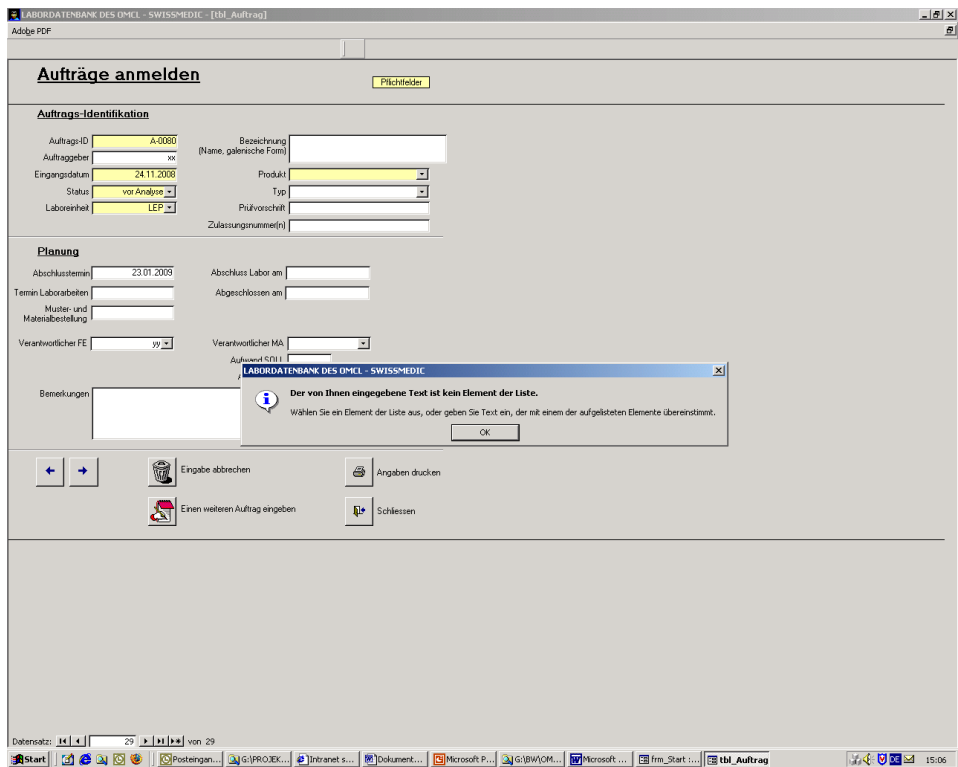


This map can be used in the specification step of a database (database structure) as well as for the design review and as documentation of this verification.

Screenshot of an input mask with mandatory fields

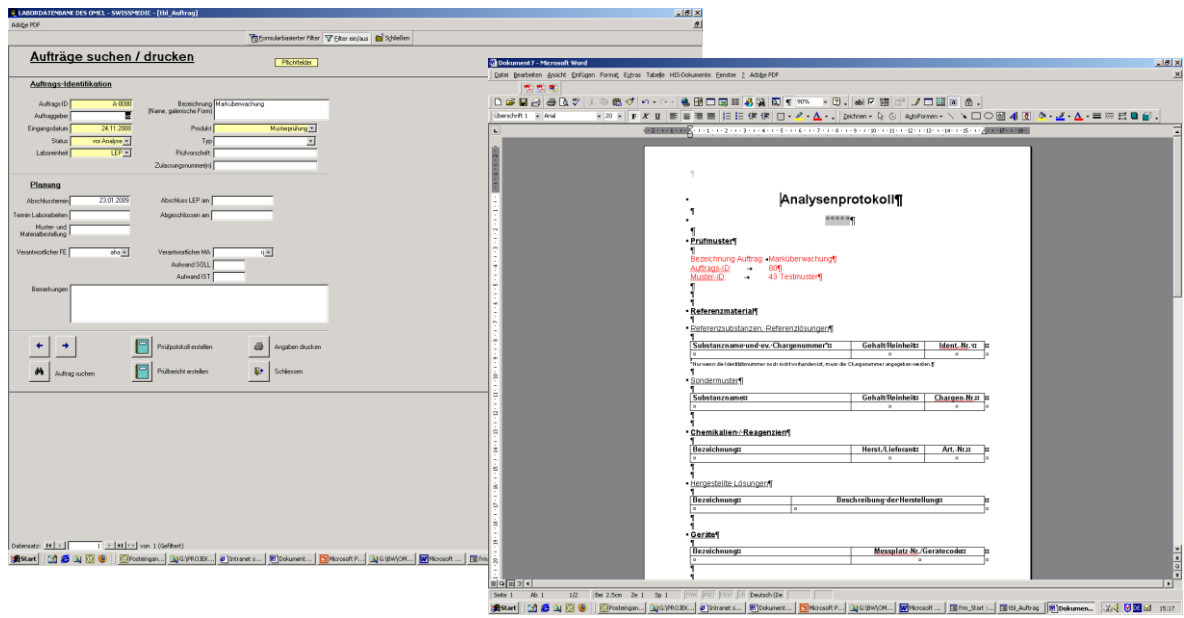
This screenshot can be used as documentation of relevant forms with the specification of mandatory fields as well as for the verification of these fields.

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)



OMCL Network of the Council of Europe QUALITY ASSURANCE DOCUMENT

PA/PH/OMCL (08) 89 R

VALIDATION OF COMPUTERISED SYSTEMS

ANNEX 3: VALIDATION OF COMPUTERS AS PART OF TEST EQUIPMENT

Full document title and reference	Validation of Computerised Systems Annex 3: Validation of computers as part of test equipment PA/PH/OMCL (08) 89 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 3 OF THE OMCL NETWORK GUIDELINE
“VALIDATION OF COMPUTERISED SYSTEMS”**

VALIDATION OF COMPUTERS AS PART OF TEST EQUIPMENT

INTRODUCTION

The present document is the 3rd 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. It is addressed to software for controlling laboratory equipment and evaluation of analytical raw data.

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.

Level I. Selection of Software and Computer Equipment

The selection and purchase of new software and the associated computer equipment should follow a conscious decision process based on the requirements for the intended use of the test equipment. Usually the first step is the selection of software which meets the analytical requirements of the intended applications. Typical requirements are listed in Table 1. In the second step, appropriate computer equipment is selected which meets all hardware requirements of the selected software. Typical requirements are listed in Table 2.

TABLE 1: ANALYTICAL REQUIREMENTS ON THE SOFTWARE

- Integration algorithms (Peak detection, identification, evaluation parameters, etc)
- Calibration algorithms
- System suitability functions (Symmetry factor, theoretical plates, resolution, etc)
- Statistical functions (mean, standard deviation, etc)
- Control of the analytical system
- User management, i.e. the administration of user accounts and the definition of user privileges.
- Electronic signature
- Compatibility to external software (LIMS, Excel, etc)

TABLE 2: HARDWARE REQUIREMENTS

- Hardware components
- Operating system
- Interfaces. Particular attention should be paid to the characteristics of the a/d converters, which may have an impact on the resolution, the accuracy, the linearity or the sampling rate.

For software and associated computer equipment already in use the user requirement specifications may be described retrospectively.

Level II. Installation Qualification

Once the software and the computer equipment are selected and purchased, the whole system should be installed and connected to the analytical instrument by appropriately trained personnel. After installation, the system should be adequately qualified. Typical parameters to be tested are listed in Table 3.

TABLE 3: INSTALLATION QUALIFICATION

- Verification that the correct operating system (incl. version and service package) is installed.
- Verification that the software controls the analytical instrument.
- Verification that the measuring signal(s) is (are) transferred to the software.
- Verification of the correct function of the user management.

Level III. Qualification of the software functionality

The proper function of the software should be checked by testing the performance of key functions like 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 vendor of the software. These raw data sets 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 spreadsheet software.

Level III Qualification should be repeated 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). Analogous behaviour should be applied for every change in hardware platform.

Level IV. Suitability for specific test procedures

In connection with the validation of an analytical procedure, calculations performed by the software of the relevant computerised system should be checked. Special emphasis should be placed on grouping of data and statistical analysis of the results. In many new software programs it is possible to implement user-defined calculations and control fields. The proper function of these parameters has to be checked by example calculations. These user-defined calculations should be locked or password protected to prevent overwriting.