eurolab
European Federation of National Associations of Measurement, Testing and Analytical Laboratories

Technical Report No. 2/2006
October 2006

Technical Report

GUIDANCE FOR THE MANAGEMENT OF COMPUTERS AND SOFTWARE IN LABORATORIES WITH REFERENCE TO ISO/IEC 17025/2005

Impression

EUROLAB Technical Report 2/2006
“Guidance for the Management of Computers and Software in Laboratories
with Reference to ISO/IEC 17025:2005”

October 2006

EUROLAB Technical Secretariat
c/o Laboratoire National de Métrologie et d’Essais – LNE –
1 rue Gaston Boissier – 75015 Paris - France
Tel.: +33 (1) 40 43 39 45
Fax: +33 (1) 40 43 37 37
Email: mailto:eurolab@lne.fr

Guidance for the Management of Computers and software in Laboratories with reference to ISO/IEC 17025:2005

Foreword

This guideline is intended to be used as an aid to laboratories when they are managing the use of software and computers with respect to the requirements of ISO/IEC 17025 [1]. The working group consisted of representatives from accreditation bodies and conformity assessment operators, specifically laboratory organisations, but also included certification bodies, inspection bodies and metrology institutes. The working group representation included the following members: Greg Gogates (A2LA), Hugo Eberhard (CEOC), Per Lang Pedersen (EA), Steve Ellison (EURACHEM), Anita Schmidt (EUROLAB), Maria Elisa Abrantes da Costa (EUROLAB), Magnus Holmgren (EUROLAB and NORDTEST, Chairman), Tanasko Tasić (EUROMET), Jan Hald (EUROMET and NORDTEST),

The terms of reference of the group were approved by the EUROLAB Technical Committee for Quality Assurance. The group started its work during autumn 2003.

1. Introduction and how to use the guide

The scope of the group was to produce a succinct and comprehensive guideline mainly focusing on managing the requirements specific for computers and software with respect to ISO/IEC 17025. This document identifies neither best practice nor a total solution, but provides advice and guidance with no mandatory parts.

It is important to accept that the introduction of information technologies – IT, computers and software into the testing and calibration processes require some interpretation. The authors identified that the overall impact of the introduction of such technologies improves the quality of a laboratory's services.

This guidance assumes that a laboratory is working in accordance with ISO 17025, i.e. has educated and trained personnel, procedures for the training and equipment maintenance, policies and procedures for the control of access and amendment of information, procedures for document control etc. Many issues concerning security, e.g. electronic transmission, of test reports is dependent more on what has been agreed in the contract between the laboratory and the client rather than what is stated in the standard.

This document reflects the situation s in which computers used in the laboratory are used in the following variety of applications:

- as simple typewriter –with all hardcopy printed and saved,
- for preparing and administering the management handbook and standard operation procedures, organisation’s structural chart, personnel data and training etc…
- for providing documents via intranet
- archiving documents
- customer databases
- control of instruments
- functionally used as an instrument
- evaluation of test results
- keeping quality control charts and calibration curves
- as intra-laboratory information and management system

- preparing test reports
- internet as external sources of information
- contacts with customers (e.g. via e-mail)
- presentation of the organisation on the website, ...

In order to apply to such a broad range of activities, the actions taken by the laboratory to control the quality of its computers and software needs to be identified and evaluated according to the degree of IT used and the risk associated with it. For this purpose this guidance offers examples in tabular form so that a laboratory can decide on the measures to be taken based on a case-to-case basis.

Activities and issues that need IT control within a laboratory's management system with respect to ISO/IEC 17025 can be grouped into two fields:

a) general activities of a laboratory that need to be controlled according to the standard in general, whether they are conducted with or without a computer system; for these activities a laboratory needs to define policies and procedures. In the case of using a computer system, this has to comply with the system requirements;

b) special requirements that have to be met for the software and systems used. Software and computer system must be validated and/or verified.

It is assumed that a laboratory will have measures to comply with the general requirements of ISO 17025. Therefore this guidance focuses on the special requirements concerning software and computer system validation, including:

- identification and interpretation of computer and software clauses in ISO 17025 (**Chapter 3**)
- implementing computing systems in the lab (**Chapter 4, 5 and 6**)
- different categories of software (**Chapter 4**)
- risk assessment including security (**Chapter 5**)
- verification and validation of software (**Chapter 6**)
- electronic documents handling, transmission and archiving (**Chapter 7**)
- references (**Chapter 8**)
- IT-adoption (**Appendix 1**)
- usage of computer networks in connection with the measurement process (**Appendix 2**)
- security (**Appendix 3**)

The guidance can be used in the following way:

Chapter 3 is an aid to help laboratories identify and interpret clauses in the standard that are directly and indirectly related to the use of software, computers, computer systems and computerised quality management systems.

Chapters 4, 5 and 6 together provide guidance in how to implement computing systems in laboratories. **Chapter 4** is a guide on how to categorise different types of software from software bought “off the shelf (OTS)“ to custom-made programmes (CMP). This chapter along with table 2 provides guidance on how to categorise software. This categorisation then helps the laboratory take decisions on the way to manage and also how to validate the software.

Chapter 5 together with appendix 3 includes a short introduction on how to estimate the risk associated with the respective software or computer system and how a laboratory can treat security issues. The proposed measures concerning security in this chapter are not directly required by the standard but are rather a collection of how to treat potential problems.

Chapter 6 tables the different types of software / computer systems and identifies related risk classes. The extent to which validation and/or tests are required before using the IT system for accredited activities are identified. The respective different types of validation and test are described in separate tables.

Chapter 7 deals with the issue of handling electronic documents.

Appendix 1 classifies the degree of IT activities of a laboratory into activities with the requirement of high, medium or low IT control requirements for the different clauses in ISO/IEC 17025.

Appendix 2 gives advice on handling networks in connection with the measurement process based on the results of the MID-Software project, which deals with handling of software and IT in measuring instruments covered by new EU directive on measuring instruments “Measuring Instruments Directive”.

Appendix 3 (together with chapter 5) deals with security issues and how a laboratory can treat them.

2. Terms and definitions

2.1 **Computing system**: A system containing one or more computers, peripheral devices and associated software products. [2]

2.2 **Verification**: Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled [3]. In this guide verification is e.g. a check of the computing system, user acceptance testing and code reviews.

2.3 **Validation**: Confirmation by examination and provision of objective evidence that particular requirements for a specific intended use are fulfilled [1, 3]. The degree of the validation needed depends on intended use.

2.4 **Electronic Record**: Any combination of test, graphics, data, audio, or any other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. [4]

2.5 **Record protection**: Assuring the authenticity, integrity and confidentiality throughout its lifetime. This includes audit trails and electronic signatures.

2.6 **Record security**: The degree to which a collection of data is protected from exposure to accidental or malicious alteration or destruction [2]

2.7 **Migration, moving of a computing system including source data from one computer environment to another**

2.8 **Record backup**: A system, component, file, procedure, or person available to replace or help restore a primary item in the event of a failure or externally-caused disaster [2]

2.9 **Electronic source (e-source), quality and technical records without maintained paper originals**

2.10 **Software product**: The complete set of computer programs, procedures, and possibly associated documentation and data designated for delivery to a user. It is deployed onto a hardware computing environment where it becomes part of the system under configuration management [2**]**

2.11 **Open system**: An environment in which system access is not controlled by persons who are responsible for the content of the electronic records that are on the system. (i.e. the internet) [5]

2.12 **Closed system**: An environment in which system access is controlled by persons who are responsible for the content of the electronic records that are on that system [5]

2.13 **Re-validation Trigger**: Software requires re-validation when either the computing system (e.g. software) or requirements are changed. Validation activities need only be focused on the relevant functions and computing interfaces

2.14 **Electronic Audit trail**: A secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record. [4]

2.15 **User session**: A finite, reasonable, period of time in which an operator is actively using a computing system. After which time the session has ended, audit trails are invoked. A change of user automatically ends the current session.

2.16 **Testing Software**: Software in a Computing System used for testing, calibration, or sampling.

2.17 **Document software**: Software in a Computing System used for managing document control, contracts management, purchasing, complaints, Non-conformances, Corrective Actions, management review, preventive actions, audits, records, proficiency trending, reports, and transmission of result.

2.18 File integrity **Check**: review of deployed software product or data files on the computing system to confirm that files have not changed (relates to ISO 17025 5.5.10 & 5.6.3.3).

2.19 **Acceptance test**: Formal testing conducted to determine whether or not a computing system meets the requirement specification and to enable the laboratory to determine whether or not to accept the system.

2.20 **Requirement specification**: The definition of what is required of a computing system in a specific intended use.

2.21 **Black-box testing**: A way to test software so that the internal workings of the item being tested are not known by the tester. Also called: Functional Testing

2.22 **White-box testing**: A way to test software with knowledge of the internal □orkings of the item being tested. Also called: Clear Box Testing, Glass Box Testing, and Structural Testing

2.23 **Role, a specific set of computing environment access rights,** e.g. user, administrator, etc.

3. Interpretation of computers and software clauses in ISO 17025

There are several clauses in ISO/IEC 17025 which may have implication on software and/or computers. The table below lists those, which could be implemented using computing systems.

Table 1 Computers and software in ISO 17025

Clause in ISO/IEC 17025	Computer, software or IT directly mentioned in the clause	Interpretation and comments
4.1.5 c	Yes	When computers are used to collect customer information it shall be secured (e.g. access via login id and role)
4.1.6	No	Electronic communication, e.g. e-mail, intranet sites etc. is consider as appropriate communication process
4.2.7	No	Applicable also for electronic management systems
4.3.1	No	Applies to documents, reports etc. in electronic format
4.3.2.1*	No	No requirements for electronic signatures only approval e.g. via knowledge management system and directory write access
4.3.2.2*	No	Not applicable as only one copy exists on intranet. Disclaimer stating un-controlled or user-controlled when printed

4.3.3.2*	No	Track changes can be used or some manual method if desired
4.3.3.4*	Yes	How to maintain documents, reference knowledge management system etc.
4.4.1a	No	Laboratory should declare the security level of its electronic transmission, both test reports and in some cases also correspondence
4.6.1	No	Applicable also for software and computers, see also 5.5.2
4.6.2	No	Applicable also for software and computers, see also 5.5.2
4.6.3	No	Applicable also for software and computers, see also 5.5.2
4.13.1.2	No	Assure that the format of the technical and quality records are readable during the whole retention period. Migration of data if necessary
4.13.1.3	No	Applicable also for electronic records
4.13.1.4 (5.4.7.2.b)	Yes	Ensure that there are procedures for back-up and for protection against unauthorised access to electronic records.
4.13.2.1	No	Normally it is not necessary to keep the old computing system for the whole retention period but to be able to show the validation evidence of the acceptability of the system at the time of use
4.13.2.2	No	Identification of the data to the assignment
4.13.2.3	Yes	Labs should identify a computer session and data changes outside the session require audit trails (i.e. data is not deleted but expired)
5.4.1	No	This clause includes software user manuals
5.4.7.1	No	Automated calculations and data transfers are verified during software validation. Further checks are not necessary until a re-validation trigger occurs.
5.4.7.2a	Yes	In addition purchased software needs acceptance testing as a check to 5.5.2
5.4.7.2b	No	See 4.12.1.4. The security when transmitting data should be considered, e.g. in contract review. Virus protection should be considered etc.
5.4.7.2c	Yes	No different than any other test equipment
5.5.2	Yes	Software/firmware fulfil user requirements through Acceptance Testing or Validation

5.5.4	Yes	Each instance of software should undergo acceptance testing in its computing environment.
5.5.5	Yes	Software should be considered as a unique piece of test equipment. The evidence of validation and/or verification should be maintained as is analogues to calibration
5.9.2	No	The quality control data may be collected and/or analysed with computer and software.
5.5.10	No	Periodic checks that software objects have not changed size or time stamp. Changes to deployed system trigger re-validation efforts.
5.5.11	Yes	Check is need only if done manually. If automatically collected via validated software none is prudent.
5.5.12	Yes	If there is an administrator role allowing all functions available it should not be used for operation. A more restricted user role for operations is preferred.
5.10.1	Yes	Reports sent to customers in electronic form shall not be editable. Use reports in locked format (e.g. pdf-type file).
5.10.2j	No	The production of electronic source reports shall be in accordance with national legislation concerning electronic signatures, e.g. pki-signature. In other situations it is preferred to have a full scanned signature page amended to the report.
5.10.7	Yes	Electronic transmission shall be encrypted unless otherwise agreed in contract review.

*) The comments to these clauses refers to the situation where the quality manual is stored in an electronic form only, e.g. as word documents on a write-protected network drive.

4. Different categories of software

Table 2 categorises different types of software in five different categories. The table contains examples of groups of programmes as well as examples of specific programmes. There are other ways of categorising software, e.g. COTS (Commercial off-the-shelf), MOTS (modified off-the-self) and CUSTOM [6], these categories are also indicated in the table.

Table 2. Different categories of software

Category	**Types**	**Groups of programmes, examples**	**Examples of programmes**
1 (COTS)	Operating systems (COTS*)	Operating systems	Windows, LINUX
2 (COTS)	Firmware, (COTS)	Embedded software, build-in software	Instruments, voltmeters, tensile testing machines
3 (COTS)	Standard software packages, Commercial off the shelf (COTS)	e-mail programmes, word processors	Word, Excel (as a table only), etc., Outlook, internet explorer, Acrobat, Stock instrument controlling software used “out of the box”.
4 (MOTS)	Configured software packages (MOTS, modified of the shelf)	Programmes as a programming and configuration environment. Tailoring & Customization is needed prior to use.	Excel formulae, Labview, Lab-windows, labtech Notebook, mathcad
5 (CUSTOM)	Custom or bespoke software (CUSTOM)	Custom written software using software programming tools. Includes Word/Excel documents with macro-code (VBA code).	Applications written in C++, SQL+, Java Visual Basic, XML, LabVIEW, LabWindows and other languages. Application may also in some cases be considered as Custom

5. Risk assessment including security

The risk connected with the introduction and use of computers, computer systems and software in a laboratory is not specifically mentioned in ISO/IEC 17025. However the level of risk affects the extent and content of the validation process and therefore it is briefly mentioned in this guide. This chapter provides only a overview of the subject and there are numerous examples of how to analyse risks in the literature.

Before new software, computers, equipment containing computers etc. are introduced in a laboratory the risk connected with such an introduction should be assessed. A risk assessment should be performed to evaluate the extent and content of validation and/or verification required. Such an assessment may include, but not be restricted to:

1) Identification of possible events which may result in a non-compliance with respect to ISO/IEC 17025 (e.g. un-correct results).

2) Estimation of the likelihood of such events.

3) Identification of the consequences of such events

4) Ways of avoiding the events (e.g. by use of check standards or reference materials in calibration/testing)

5) Costs, drawbacks, benefits etc. occurring when the ways in 4) are chosen

6) Analyse the consequences of the things in 5) together with 3)

7) Decision on activities

8) Office or Testing Software

In a laboratory the risks are in many cases associated with the results of tests and calibrations and the use of such results.

The outcome of the risk assessment is used to determine the extent of the validation of both software and test and calibration methods.

There are few clauses in ISO/IEC 17025 that specifically require laboratories to have procedures etc. for computer and IT-security. Clauses 4.13.1.4, 5.4.7.2 b and 5.10.7 and they are dealt with in table 1. However many laboratories need broader guidance in these matters and therefore this chapter gives some advice concerning security etc.

The table in appendix 3 indicates the typical precautionary measures expected for different levels of security requirement. Note that ‘security’ in this context includes integrity/accuracy issues.

The table in appendix 3 considers integrity (essentially, the data accuracy requirements) and availability as separate issues. Precautionary measures are grouped by ‘requirement’; the measures considered appropriate becoming more stringent as the security requirement increases from low to high. The ‘examples’ under each of these sections provide an illustration of scenarios, which might be considered to fall into each category.

In most cases, as the requirement increases, risk can be controlled either by adopting substantially more stringent procedures or by adopting combinations of measures. For example, a combination of physical access control and ordinary password protection may be as effective in practice as biometric identification with less stringent physical access control.

Different measures may be more or less important depending upon individual circumstances. For example, very short reporting deadlines in a testing laboratory may mandate far higher levels of hardware redundancy and repair and maintenance service than would be expected from the criticality of the data alone.

Where IT systems are critical to a business, unauthorised changes should be prevented by access control (e.g. password protection or physical access security). Where critical systems are not protected in this way, users are recommended to confirm and document the status of the configuration before use of the system.

Finally, it is most important that all staff are aware that the procedures are in place and must be followed. Introduction of new personnel and/or staff training will require each person to be provided with information and training on IT security issues. Staff should be made aware of their responsibilities.

The level of security required when reporting results electronically from tests and calibrations should be discussed with the customer as a part of contract review. Integrity and confidentiality are dependent on the contractual agreements. In fact security is dependent on an agreed contract or found during contract review.

6. Verification and validation of software

The validation/verification of software is dependent on whether it is bought or custom built. The extent of effort required should be based on risk assessment. Purchased software should be checked (verified) to confirm it usability in the user environment. This is typically evident by acceptance testing against manufactures specifications and/or user requirements.

Custom built or modified software shall be validated to the extent necessary. The table 3 provides guidance.

Table 3 Test and validation of software

IT-risk **Software category**	**Low**	**Medium**	**High**
Category 1 Operating systems (COTS)	No test of OS itself. New acceptance test of med/high risk SW in category 4-5 after OS upgrade.		
Category 2 Firmware (COTS)	No validation	SW is part of equipment, which must be tested/calibrated according to ISO17025, 5.5.2. This could include e.g. validation V1, V4 and tests T1, depending on the actual equipment.	
Category 3 Standard software packages (COTS - Commercial off the shelf)	No validation	Check input/output for consistency (e.g. peer review of documents). Example: word processor used for writing testing reports.	Validation V1,V4 Tests T1-T2

IT-risk —————— **Software category**	**Low**	**Medium**	**High**
Category 4 Configured software packages (MOTS)	Check input/output for consistency (e.g. peer review of documents).	Validation V1,V4 Tests T1-T3	Validation V1-V5 Tests T1-T4
Category 5 Custom or bespoke software (CUSTOM)	Validation V1,V4 Tests T1	Validation V1-V5 Tests T1-T3	Validation V1-V5 Tests T1-T5

The validation phases V1-V6 refer to the different phases in a typical validation plan based on the software lifecycle, as shown in the table below. The lifecycle validation plan integrates the validation and the software development process. The software developer is responsible for the phases V2 and V3, and the end user is responsible for the major part of the phases V1, V4, and V5.

	Table 4a. Validation phases
V0	Manufactures documentation
V1	Requirement specification
V2	Design and implementation (coding)
V3	Inspection and structural testing (“white-box” testing)
V4	Installation
V5	Acceptance test (“black-box” testing)
V6	Operation & maintenance (in the text)

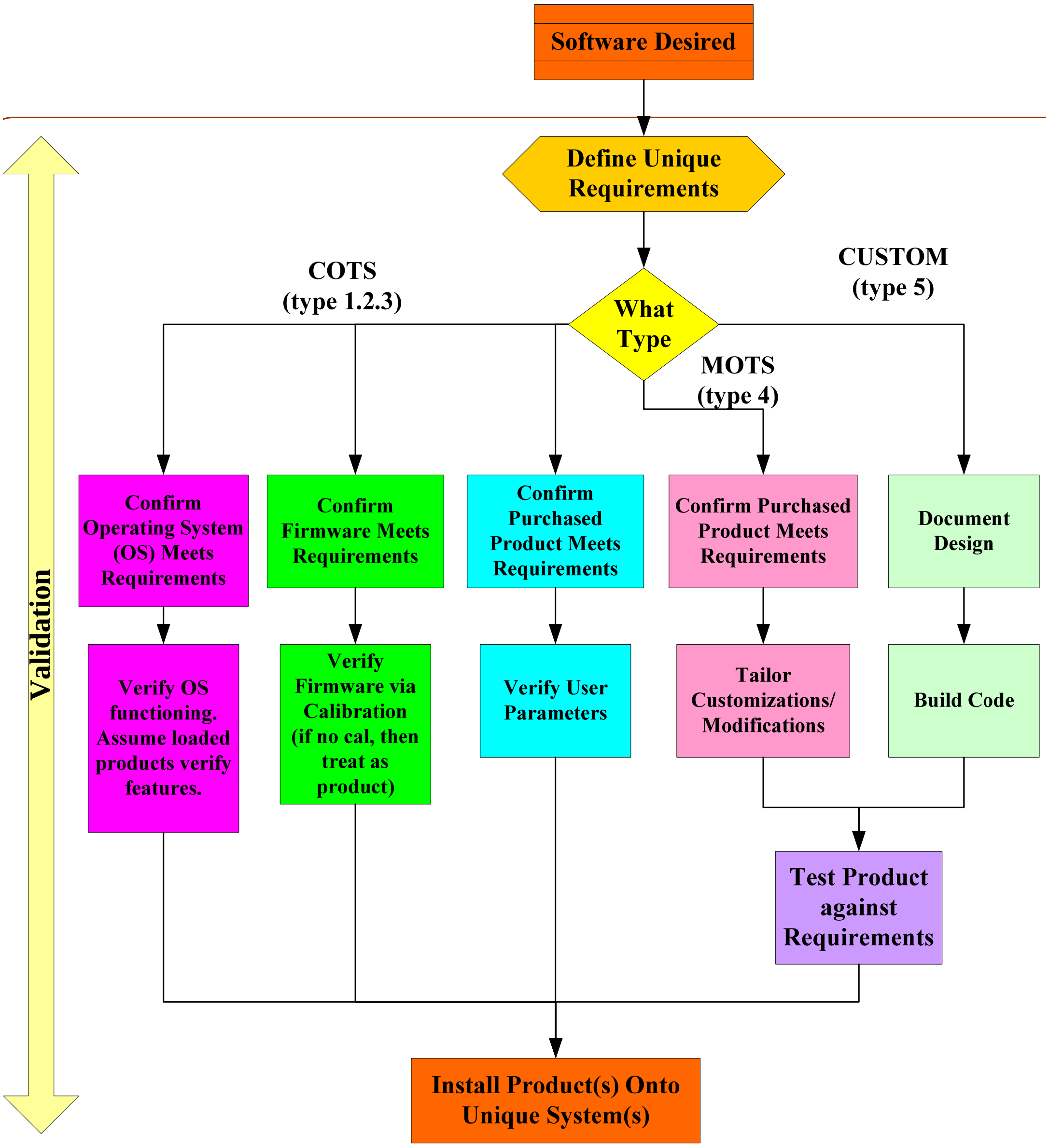
The different types of black-box tests (T1-T6), which enter in table 3, are specified in table 4b. This table includes examples of typical black-box tests used in software validation, but the list is not exhaustive.

	Table 4b. Black-box tests
T0	**Manufacturers specification**
T1a	Typical input data set, check for obvious errors in produced output
T1b	Test of data transfer by direct observation, e.g. from instrument to data file under typical operating conditions.
T2	Test of SW functionality, in particular with respect to integrity, traceability, access rights, safety etc.
T3a	Typical input data set, where produced output is checked against a ‘parallel’ processing of data (e.g. manual calculations, reference software).
T3b	Calibration of ‘known’ standards (e.g. with a history or by intercomparison)
T3c	Generation of typical test data set with known output result
T4a	Generation of data set for boundary value analysis[i]
T4b	Generation of data set with unexpected values (extreme input data)
T4c	Test of data transfer under extreme conditions, e.g. where instruments or SW are stressed
T5	Testing with usage of simulation of particular devices.

According to ISO17025, 5.4.7.2 all software used for handling calibration or test data must be validated, except for software in categories1-3 in table 2, where the “validation” is limited to an acceptance test. However, all software used for testing or calibration shall be capable of achieving the accuracy required and comply with relevant specifications. Thus, validation phases V1 and V4 must be completed even for software in category 3. The level of validation depends on the software type and its application. Other validation reports as well as any history of error-free operation may be included as part of the laboratory validation of a software product.

The verification and/or validation procedure presented above is presented in more detail in [7].

Figure 1 shows the different paths, depending on the software category, for introduction of new or revised software in a laboratory. It is clear that new versions of software need to be checked/validated before introduced in the laboratory. The extent of the validation depends on the software and its use as well as on the risk connected with its use.


Software Desired
Define Unique Requirements
Validation
COTS (type 1.2.3)
What Type
CUSTOM (type 5)
MOTS (type 4)
Confirm Operating System (OS) Meets Requirements
Confirm Firmware Meets Requirements
Confirm Purchased Product Meets Requirements
Confirm Purchased Product Meets Requirements
Document Design
Verify OS functioning. Assume loaded products verify features.
Verify Firmware via Calibration (if no cal, then treat as product)
Verify User Parameters
Tailor Customizations/ Modifications
Build Code
Test Product against Requirements
Install Product(s) Onto Unique System(s)

Configuration Managemer

Figure 1. Different paths for introduction of new software in a laboratory.

Clause 5.4.7.2 a in ISO/IEC 17025 should not be interpreted as that it is allowed to use software without any checks/validation if it is developed by another organisation than the laboratory. From 5.5.52 it is obvious that the some sort of check/validation/acceptance test has to be performed for such software before it is used in the daily activities. The main responsibility for the checks/validation and the way it is performed may be an issue for contractual agreements between the developer and the laboratory. However a laboratory holds the main responsibility for the state of its equipment (including software).

Some User Acceptance or Testing is required to satisfy this requirement. Custom Legacy systems prior to invoking this guidance, can be construed as purchased software only until it requires modification. At that time it reverts back into custom and requires validation.

It is very important that all validation, changes, versions and key comparisons are documented contemporaneously. Changes made to IT hardware and software including application programmes should be documented (e.g. in a local log book).

The information may include who made or authorised the changes, the date and reason, together with tests made to confirm correct operation.

Many laboratories frequently use spreadsheets, e.g. excel, in their daily activities. Depending on the extent of programming they should be validated as category 3 (COTS) or category 4 (MOTS) software. The following guidance is given regarding spreadsheet layout:

- use colouring or shading of cells to distinguish status,
- lock cells that are not for input data,
- protect worksheets and workbooks by password,
- provide operator instructions on the worksheet which takes input data or on their own worksheet
- set the format of cells appropriately for the data that is to appear in them.

The following spreadsheet parameters can be checked/tested if applicable:

- the implementation of the calculations is correct,
- repeated calculations have been correctly copied,
- rounding has been done at the appropriate place in the calculation,
- accuracy of calculations using standard or reference test data,
- correct treatment of parameters by using test data with values of the parameters in range, on the edge of the range and outside the range of allowed/expected values.

7. Electronic documents, handling, transmission and archiving

Several of the issues concerning electronic documents have already been mentioned e.g. in table 1. A general comment is that there should not be any major differences in the requirements for laboratories using electronic documents compared to laboratories using paper documents. However, it must not be forgotten that the introduction of electronic documents is open to both special opportunities as well as specific problems and there are some clauses in ISO/IEC 17025 that mention handling, transmission and archiving of electronic documents. Clause 4.13 “Control of records” contains several clauses of special interest for those using electronic documents. Examples of issues mentioned are the need for back-up, audit trail, mistakes in records and retaining of records. But these clauses are clear and together with table 1 there should not be any problem with the interpretation.

In the standard there are very few requirements for actual signatures of documents. One example is clause 4.13.2.3 where there is a requirement that changes in records are signed or initialled. It is also useful to date changes. In electronic documents this can be dealt with access rights and by clearly marking the change with a note of who made the change. This is called audit trails and is an electronic version of the traditional cross-out/initial/date technique used in the paper world.

There is also a requirement for signatures or equivalent is in chapter 5.10.2 “Test report and calibration certificates”.

This can be dealt with by using a “real” electronic signature using standard PKI (public key infrastructure) techniques (this is a good solution when the report/certificate has legal implications) or by scanning the executed “wet-ink” signature page and saving in a secure locked format such as PDF.

Electronic transmission of test reports and calibration certificates should be encrypted if not otherwise is agreed in the contract or the contract review. In general electronic communication with the customers there may be rare cases that lead to an increased risk of the information to end up in the wrong hands. For normal laboratory activities this is not likely and security measures taken should be appropriate for the actual risk.

When electronic documents are retained and archived, take measures to ensure that they are retrievable during the whole retention period. Techniques would include migration to new media and/or re-saving into new future formats.

8. References

[1] ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories

[2] IEEE Std 610.12-1990 IEEE Standard Glossary of Software Engineering Terminology -Description

[3] ISO/IEC/IEA/IEEE 12207:1996 “Information Technology – Software Lifecycle Process”

[4] US FDA Guidance for Industry, “Computerized systems used in clinical trials: 2001”

[5] Draft FDA Guidance for Industry “21CFR part 11: Electronic records; Electronic Signatures Validation”, 2001

[6] Gregory D. Gogates, “Software Validation in Accredited Laboratories A Practical Guide, Fasor, Landsdale Pennsylvania, 2001

[7] Carl Erik Torp, “Method of Software Validation”, NT Technical Report 535, Nordtest, Helsinki 2003.

Other documents of interest :

* ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management

* The GAMP Guides e.g. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture – GAMP 4.

- ISO/IEC 121119:1994 Information Technology – Software Packages – Quality Requirements and Testing”

- The WELMEC Guides, e.g. WELMEC 7.1 Issue 2 Development of Software Requirements and WELMEC 7.2 Issue 1 Software Guide (Measuring Instruments Directive 2004/22/EC)

- Measuring Instrument Directive 2004/22/EC

- Directive 95/46/EC Personal Privacy

- ISO/IEC Technical Report 13233:1995 - Information Technology – Intrepretation of Accreditation Requirements in ISO/IEC Guide 25 – Accreditation of Information Technology and Telecommunication Testing Laboratories for Software and Protocol Testing Services.

- ADCM - Computer Systems Validation in Clinical Research - A Practical Guide (Edition 2):2004

Appendix 1. IT-adoption

Table A.1 provides examples of the use of IT systems in laboratories accredited to ISO/IEC 17025. The intent is principally to indicate the general level of implementation and management practical control considered advisable for different IT implementations. In some sense this can also be interpreted as IT-risk

	Table A.1. The use of computer and software leads to the following IT-adoption			
17025 and other possible requirements/needs	**Low IT-control requirement**	**Medium IT-control requirement**	**High IT-control requirement**	**Comments**
1-3				Not of interest
4.1 Organisation	Paper systems for organisational management and documentation; IT only used in generating paper for permanent record.	Records retained or accessed primarily via IT systems, but hard copy forms definitive record or is always available.	Records maintained only on IT systems; authority assignments rely on IT applications. Scheduling etc rely heavily on IT applications. Personal information held on IT systems.	Appoint a responsible person for the computer system. Risk depends of the complexity of the system
4.2 Management System				See document control
4.3 Document control	Purely paper system. IT only used to produce the papers	Records retained or accessed primarily via IT systems, but hard copy forms definitive record or is always available.	Fully computerised system for quality documentation management, authorisation and version control.	Availability main problem. Watch out for the access to the electronic versions. See sections 4.3.2.2.a & 5.4.1 It is important to also control write access.

17025 and other possible requirements/needs	Low IT-control requirement	Medium IT-control requirement	High IT-control requirement	Comments
4.4 Review of request	Paper system; no electronic copy or production	IT used to collate information, generate paperwork etc.	Electronic transmission of commercially sensitive issues, to be discussed with the customer. .	Commercial confidentiality leads to significant IT risk and will generally require some security precautions even for word processor systems to maintain confidentiality.
4.5 Sub-contracting	Paper reports only	Electronic version of paper reports is important for customer reporting; Raw data transferred for further analysis.	Raw data and/or reports generated, transferred and used automatically to generate reports directly to customers.	Format of the data has to be agreed. Integrity checking for electronic data is important. Commercial confidentiality adds confidentiality control requirements.
4.6 Purchasing, services and suppliers	Buying a standard PC for administrative purposes	IT used to report on measurement results; IT used to control and acquire measurement results from isolated instruments	IT used generally for data acquisition, processing and reporting; LIMS-systems	Acceptance test.
4.6 Purchases Services			The level of control is dependent of the size of the system end the dependence on the subcontractor.	IT subcontractors must sign confidentiality statement. Service level agreement is essential.

17025 and other possible requirements/needs	Low IT-control requirement	Medium IT-control requirement	High IT-control requirement	Comments
4.7 Services to the customer				None
4.8 Complaints As 4.11	Paper systems; IT used to generate paper for records etc.			Access problem may occur. Have the complaint really been handled.
4.9 Control of non-conforming testing work	Paper systems; IT used to generate paper for records etc.	IT systems used as support for identifying out-of-control conditions. Records held on paper file as well as IT	IT forms the sole method of identifying defects Records held only on IT systems	
4.10	Paper systems; IT used to generate paper for records etc.	IT systems support supporting the identification of possible improvements in larger organisations IT used to support improvement decisions or analyse data for information.	IT system is sole means of identifying possible improvements. IT used to identify appropriate action	
4.11 Corrective actions	Paper systems; IT used to generate paper for records etc. IT systems used to track corrective actions at low frequency and/or in small areas.	IT systems support tracking of corrective actions across larger organisations. IT used to support corrective action decisions or analyse data for information.	IT system is sole means of tracking corrective action. IT used to identify appropriate action	

17025 and other possible requirements/needs	Low IT-control requirement	Medium IT-control requirement	High IT-control requirement	Comments
4.12 Preventive actions	Paper systems; IT used to generate paper for records etc.	IT systems support planning of preventive actions across larger organisations IT used heavily to support corrective action decisions or analyse data for information.	IT systems form sole records, sole source of defect tracking etc. Management review relies solely on IT.	
4.13 Control of record				See Document Control
4.14 Internal audits		Planning	Planning	
4.15 Management reviews	Non-sensitive information (not personal or commercially sensitive) held on IT systems and used for review.	Some sensitive information held on isolated IT systems; significant dependence on IT-generated statistical information.	Management review relies solely on IT-based information. [Rare]	Managers rarely rely solely on IT systems for management review.
5.1 General technical requirements.				None
5.2 Personnel	Not applicable	IT systems used in generating paper records.	IT systems used to store any personal information, such as salary, home contact details, or medical information.	i) Use of IT for personnel records management is often subject to national legal requirements concerning the use of personal data. Legal requirements must be met. ii) Access control for due confidentiality is probably the most important issue for personnel records. Integrity (to prevent unfair treatment) is also important but this can usually be checked periodically with the individuals concerned.

17025 and other possible requirements/needs	Low IT-control requirement	Medium IT-control requirement	High IT-control requirement	Comments
5.3 Accommodation and environment	Not applicable	IT monitors environment and informs environmental control decisions.	IT used to control laboratory environment in critical areas (e.g. temperature or humidity conditioning areas, test chambers etc)	
5.4 Test methods and method validation	Not applicable	IT systems used for generating paper copies of test methods. IT systems used to perform calculations used in validation.	Test methods solely in IT systems (LIMS)	Ensure that electronic document control provides "readially accessible" methods.
5.5 Equipment	Electronic system only performs simple operations as directed by the operator and produces raw data for subsequent treatment.	IT system used to control isolated equipment or equipment of closely similar type; IT system processes data and generate results for subsequent reporting. Experienced operator supervision. Configuration control	IT system controls several items of equipment or collates and/or processes data from several different equipment types. Equipment run solely via IT and reports generated with minimal operator supervision Configuration control	IT systems "significant" to testing is considered equipment and must be validated or verified prior to being placed in service.

17025 and other possible requirements/needs	Low IT-control requirement	Medium IT-control requirement	High IT-control requirement	Comments
5.6 Measurement traceability	No calibration data held on IT systems. Calibration data input directly from paper records to support result production in simple calculations.	Complex IT based calculations use calibration data from a variety of sources including paper. Subject to operator supervision.	Calibration data held solely on IT systems and used automatically in producing results and placing traceability information on reports.	
5.7 Sampling	IT systems not used, or only used to produce paper sampling plans and record sheets.	IT systems used to plan sampling using geographical or other data IT used in automatic recording of sampling information (time, location etc)	IT systems control physical sampling and provide all relevant records.	
5.8 Handling of test items	Not applicable	IT systems used for parts of sample handling/ tracking (e.g. label production, numbering)	All sample handling information and tracking held on IT systems (LIMS). Fully automatic sample handling systems driven by external IT	
5.9 assuring the quality of test results				None
5.10 Reporting of the results	Not applicable	IT used to generate reports for checking and signature.	IT generates reports electronically Large scale generation of routine reports on paper	

Appendix 2 MID and usage of networks in connection with the measurement process

This appendix is based on the results of the MID-Software project, which deals with handling of software and IT in measuring instruments covered by new EU directive on measuring instruments “Measuring Instruments Directive” and is not a requirement of ISO/IEC 17025).

Distributed measuring systems (transfer of measurement data from remote instruments, remote operation of measuring instruments)

a) **Closed network**

In case of closed networks the situation is not so critical.

b) **Open network**

In a network with unknown participants it is necessary for the receiver to identify the origin of a message without ambiguity. Unforeseen delays are possible during transmission. For a correct assignment of a received measurement value to a certain measurement the time of measurement must be registered.

That means each measuring value:

- ID of measuring instrument,
- ID of measurement,
- time stamp included,
- signature of the message (CRC, digitally signed hash or whole message)
- encryption (disputable, depending on the risk) of the measurement data.

During evaluation:

- check that software on transmitter side performs these functions.
- check that software on receiver side checks these functions.

Data that are detected as having been corrupted must not be used.

Keys and accompanying data: (handled in some other part of the document)

The measurement must not be inadmissibly influenced by a transmission delay. Transmission disturbances happen accidentally and cannot be excluded. The sending device must be able to handle this situation. The reaction of the instrument if transmission services become unavailable depends on the measuring principle. Measurements that are not interruptible, e.g. the measurement of energy, volume, etc, do not need a special intermediate buffer because these measurements always are cumulative. The cumulative register can be read out and transmitted at a later time when the connection is up again.

Download of software (e.g. bug-fixes, updates, new applications, etc to measuring instruments)

Communications links may be direct, e.g., RS 232, USB, over a closed network partly or wholly control, e.g. Ethernet, token-ring LAN, or over an open network, e.g. Internet.

- The instrument should be capable of detecting if the download or installation fails. A warning shall be given. If the download or installation is unsuccessful or is interrupted, the original status of the measuring instrument shall be unaffected. Alternatively, the instrument shall display a permanent error message and its metrological functioning shall be inhibited until the cause of the error is corrected.

- During download and the subsequent installation of downloaded software, measurement by the instrument shall be inhibited or correct measurement shall be guaranteed.

- The number of re-installation attempts shall be limited.

- Means shall be employed to guarantee that the downloaded software is genuine.

Before the downloaded software is used for the first time, the measuring instrument shall automatically check that:

- The software is authentic (not a fraudulent simulation).
- The software is approved for that type of measuring instrument.

It shall be guaranteed by appropriate technical means that downloads of legally relevant software is adequately traceable within the instrument (system)

It shall be guaranteed by technical means that software may only be loaded with the explicit consent of the user or owner of the measuring instrument, as appropriate.

Some requirements/recommendations for hardware
The presence of a defect may or may not be obvious. Whether the defect is obvious or not, the presence of a significant fault should be detected by the measuring instrument itself.

Appendix 3 Security

This table is showing different aspects of security in connection with the use of IT in laboratories.

Table A.3				
Availability				
Requirement:	**Low**	**Medium**	**High**	**Remarks**
Examples:	Permanent loss of IT-held data unimportant (e.g. because paper systems exist and are reliable). Temporary unavailability over weeks is not critical.	Permanent data loss causes significant credibility loss or substantial additional work to re-enter/ reconstruct. System unavailability over 1-5 days not critical. Down time of 1-5% not critical	Permanent data loss may cause overall business failure. System unavailability critical over hours or less.	
Typical Control measures				
Storage	Single storage system (e.g. local hard disk) with original software retained for rebuild.	Single primary storage system (hard disk, network server)	Multiple redundant storage systems (mirrored, RAID etc). 'Hot-swappable' storage.	Backup requirements depend on acceptable loss timescale (e.g. if half a days' work may be critical, back up at least every half day)

Recovery	Backup at user discretion (e.g. when a report is in progress and loss might cause delay in reporting).	Daily to weekly backup system in place. (Hierarchical backup system recommended. Note 1) Local backups held in secure/fireproof location. Data is stored off site at least weekly.	Fully automated incremental backup over hours. On-line remote backup. Off-site secure storage.	
Migration of data		Proprietary software for data storage may cause troubles migrating data.		
Backup media	Magnetic media	Magnetic media with appropriate lifetime retained in appropriate storage conditions; Magneto-optical media.		Media depends on required storage life.
Hardware redundancy	None	*Either*: Secondary system identified for emergency use (e.g. a second PC or server which can be temporarily adapted as a replacement) *or* rapid hire/ replacement arrangement available	Multiple redundant systems (e.g. duplicate fileservers with ‘failover’ capability)	
Maintenance and repair	Limited Manufacturer warranty cover; ‘return to base’ cover.	On-site repair within 1-3 days	On-site repair within four hours	

Integrity				
Requirement:	**Low**	**Medium**	**High**	**Remarks**
Examples:	Errors in data are not critical. Numerical accuracy is not critical (e.g. 2-significant figures sufficient) Note: measurement data are never in this category for an accredited laboratory	Errors in numerical values have impact for customers. Errors in other data have significant customer or other business impact (e.g. incorrect reporting etc). Ordinary numerical precision is sufficient (e.g. 6-8 significant figures are sufficient) Note: most calibration and testing data fall into this category.	Errors have safety- or health-critical impact. Results are used in criminal proceedings. Numerical accuracy over 8 significant figures is significant.	
Typical Control measures				
Software verification/validation	**See table 3**			
Access control	Controls should ensure that users have sufficient familiarity with IT systems or instructions are readily available.	Access controls must be in place to ensure that staff is duly trained to use the systems and their skills adequate.		

Procedures	System and software ‘help’ systems and/or manuals are generally sufficient.	System and software ‘help’ systems and/or manuals are required and should be supported by documented instructions (which may be electronic) for specific calculations /procedures using the software.	All data entry and calculation must follow detailed documented procedures	Note: All systems should have appropriate documented usage procedures in any accredited laboratory
Software configuration	Software may be installed by users with permission.	The software installed should be documented (a software change log is generally sufficient). Software changes of any kind should be managed and undertaken by suitably qualified and experienced personnel with authorisation.	Software should only be installed after thorough testing for compatibility with system and other software. Formal procedures for authorisation for any configuration change should be in place.	1. Measures should always be taken to prevent accidental or deliberate installation of malicious software. 2. Applicable software licensing and copyright laws must be respected at all times.
Down load of software		Policies for download and installation of software must be implemented. Example Windows 2000 service pack 4.		