DANAK's retningslinie for anvendelse af computere til teknisk prøvning.	Nr.: Dato:	RL 10 1999.12.07

Link to DANAK copy

Bilag 1

Document: EA Guidelines for the use of computers
EA/GA(98)95
and computer systems in accredited laboratories
Issue: Version 4
Date: May 1998

This Guide has been developed by EAL Committee 3 (Sectoral Committee) in co-operation with EUROLAB. No final consensus could be reached on the final text. Moreover, the revision of EN 45001 and ISO/IEC Guide 25 will necessitate a number of amendments. Therefore it has been decided to continue with the development of the guide as soon as ISO/IEC DIS 17025 has been approved. As there is a need for guidance on the subject and as the guide in its present form contains material that laboratories might wish to use, EA has decided to add this introduction to it and to publish it in this form and not yet in the approved (yellow) series. The document in its present form is for information and is not intended or suitable for assessors to use as criteria document.

1 Contents

2 Preamble

All parties using this guide should bear in mind that this document covers only the accredited activities of the laboratory and only to the extent to which computers and computer systems have an influence on the quality of the accredited work performed. In doing so, it should not be the complexity of the instrument or system that is used as a measure to include or exclude the use of this guide. Decision should be taken judging from whether the instrument or system processes data acquired by measurements and tests within the scope of accreditation of the laboratory.

This guidance document is written to cover the needs of all laboratories independent of size and field of activity. The guidance given may therefore be implemented at different levels of detail for different laboratories. In some cases it might be appropriate to find simpler solutions and in others the guidance might be redundant due to the size or type of the activity in question. How the guide is implemented depends on the risks the laboratory is exposed to. Thus, it follows that a risk analysis is a fundamental issue when implementing this guide.

Whenever these guidelines are used, whether it is by a laboratory or an accreditation body special care should be taken, in each individual case, to consider the relevance of applying these guidelines. In doing so, consideration should be given to whether the computer system in question affects the quality of the accredited work to be performed by the laboratory.

Computers and computer systems are gaining wide use in accredited and applicant laboratories. Such systems include computers, automatic measuring and test systems, instruments with embedded computers, etc. When an accreditation body assesses a laboratory for the first time there is often a computer or an automatic measuring or test system already in function in the laboratory. More often than not, these have been in use for some time at the laboratory and the laboratory does not always have the possibility to go back to the supplier of the system to require supplementary information or help with the verification of the system. It is also common that a laboratory wishes to know how to meet the requirements for accreditation with respect to an automatic measuring and test system before acquiring it. This document is a guideline for laboratories aiming to meet the requirements of EN 45001 and/or ISO/IEC Guide 25 with respect to their activities where computers and computer systems are incorporated. EN 45001 and ISO/IEC Guide 25 describe the requirements on laboratory work involving testing, calibration and sampling both in laboratory premises and at other locations, for example site testing. Many of the requirements of these two documents have been easily applicable to laboratories either directly or after providing guidance in special technical fields. Before this guide was produced, there were no guidance documents for the application of the requirements of accreditation to computers,

computer systems and instruments with embedded computers.

Within the framework of the third OECD Consensus Workshop on Good Laboratory Practice held in October 1992, a group of experts discussed the interpretation of the GLP Principles as applied to computerised systems. This work was later on continued and the results were published in 1995 in a document called "OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, Number 10; GLP Consensus Document - The Application of the Principles of GLP to Computerised Systems; Environment Monograph No. 116". This document has been compared with the present guidelines. The major difference between the two documents is one of terminology where the GLP document uses specific GLP terms like "study directors". The only term that is different in the two documents and is of substantial value for our understanding is validation. The GLP document No.10 uses the term validation throughout while the EA guide uses the term verification throughout. However, with the explanation that is provided in Chapter 4 of this guide, there will not be any confusion.

Neither simple word processors nor pocket calculators constitute acceptable exceptions in general. Misuse of word processors, for example by creating reports directly from prior reports, introduces several risks, and the use of these systems needs to be appropriately controlled. Pocket calculators are sparse in numerical precision and memory, and the resulting compromises require some care in use. A classic example is the standard deviation of data with high dynamic range, which is often reported as zero due to internal rounding errors. However, issues of this type are not specifically treated in this document, as these constitute part of the general risk analysis to be carried out by the user.

Computer systems should be operated to maintain adequate integrity of data, confidentiality and availability of systems. The most difficult question is what constitutes "adequate". This cannot be answered simply for all systems. Laboratories should therefore place stress on assuring that systems are controlled according to a realistic assessment of risk to the particular system before deciding on particular measures.

One of the most critical areas for accreditation is data integrity – ensuring that the data is an accurate representation of the results of work done. Customers of accredited laboratories typically expect confidentiality, taking data integrity as given. Laboratories themselves tend to focus on availability – the system must be operational at the right times. It is, of course, the duty of the laboratory to see that customer confidentiality is respected and that the integrity of data is assured. The delivery of an effective service will necessarily require the laboratory to attend to confidentiality and availability issues. Any issues of system security or IT security should cover the full range of measures required to control all relevant risks to data, not just confidentiality issues.

3 Scope

3.1 The guidelines given in this paper are applicable to accredited laboratories using computer systems, including computers embedded in other equipment or systems, where such use could affect the integrity, security, quality, accuracy and reporting of test and measurement results of those laboratories.

Some examples are:

1. Data acquisition, processing, transfer and storage;

2. Word processing where this incorporates data acquired during measurements and tests;

3. Laboratory information management systems;

4. Microprocessor controlled instruments or systems;

5. Data handling or processing systems, integration systems;

6. Computer controlled equipment or systems.

The guidelines cover all systems whether proprietary or developed in-house, and also any modifications, 'tailoring', programming, or other configuration whether undertaken by system suppliers, third parties or any staff within the laboratory. In particular, the issue of end-user programming through 'macros' or other automation facilities is becoming increasingly important and need looking into.

3.2 There are cases where test equipment that can be characterised as a computer system is used as a single entity, sometimes called black box. In these cases it is not always relevant to break the system down into its individual components, as this would not substantially add to the quality of the work. An accreditation body should take this into consideration in each individual case before deciding whether to apply this document to that particular case.

Very often, reasonable assurance of correct operation for a particular task is attained by observation of the complete system operating in situ over a period of time. Indeed, such assurance cannot be obtained without testing the complete system in practice. It follows that for many practical purposes, testing individual system components is neither necessary nor sufficient. However, it is important that such "black box" tests cover the full range of cases likely to be encountered and that the practical limitations of the system are established.

4 Explanation of terms used in this guide

4.1 Computers and computer systems

The terms **computer** and **computer systems** are used for the hardware, software and firmware that together make up the computer-based equipment used in a calibration or test, or for any other computer being used. This includes equipment connected to a computer network. In what follows, this is addressed as "the system".

The phrase "connected to a computer network" might seem to imply that the network itself is excluded from "the system". Clearly, if the network forms part of the data transmission pathway, it becomes part of the data processing system and, as with other data transmission media, there may need to be evidence of accurate and secure operation. In many systems, considerable calculation work is done in third-party packages such as spreadsheets. It is worth stressing the point that these would be considered as part of "the system".

4.2 Software
The term **software** is used for the intellectual creation comprising the programs,

procedures, rules and any associated documentation pertaining to the operation of a data processing system.

4.3 Firmware

The term **firmware** is used for the computer program(s) held in a permanent form within a computer.

4.4 Hardware

The term **hardware** is used for the mechanical, magnetic, optical and electronic design, structure and devices of a computer. Thus, hardware is the physical equipment as opposed to programs, procedures, rules and associated documentation.

4.5 Raw data

The term **raw data** is used for data that cannot be derived or recalculated from other information.

4.6 Throughout this document the term verification has been used. The activities performed to prove the quality of the software to be used after its initial manufacturing would normally be called **validation**. If we consider this as an "initial verification of the software" the term verification can be used throughout the document. The term **verification** is used for all the activities to be undertaken in order to prove that the system or any parts thereof meet the agreed specifications and perform satisfactorily in the applications for which it is being used.

5 Organisation and management

5.1 In many organisations a computer system is accessible by entities, i e people, organisations or machines, not included in the accreditation. All access should be properly authorised and duly controlled.

5.2 Basically, the system used within the accredited activities should be under the control of the accredited laboratory. If the laboratory has to share a system with other parts of the organisation, this should be done in such a way that any changes introduced to the system from other parts of the organisation do not affect the part of the system used by the accredited laboratory. These are reasonable requirements but may become increasingly difficult in practice as outsourcing, remote facilities management and distributed data systems become more common. For example, a third party support company will operate their own quality systems for change control. The responsibility of the laboratory is to ensure that where services are carried out outside direct control of the laboratory, contractual or other controls exist to ensure integrity.

5.3 The laboratory should appoint a person or persons responsible for the management and supervision of the computers or computer systems. The persons appointed to manage and supervise the system should have authority to make decisions concerning the system in question and at least the following qualifications:

- Expert knowledge necessary to use the system without threatening the integrity or security of the results of the calibrations or tests;

- Experience necessary to determine whether the documented procedures used with the system are adequate for their purposes;

- Knowledge and experience to judge whether a change to be incorporated is of a type that can cause damage to the system or jeopardise the quality of the work of the laboratory.

It is inevitable in small laboratories that one person will have all responsibility for a system. However, for critical systems, it may be essential to separate elements of authorisation, security, system administration functions and/or data entry and modification capabilities. In particular, it is a principle of some auditing practices that authorisation and execution responsibilities should be separated to reduce risk of fraudulent activity. In IT security, errors are probably most likely to arise where a change is suggested, specified, approved, implemented and authorised by a single individual even though this may be necessary in practice.

5.4 The laboratory should define the following areas of responsibility as appropriate:

- Specification,

- Design,

- Acquisition,

- Installation,

- Testing,

- Acceptance,

- Maintenance,

- Modification,

- Decommissioning,

- Security,

- Administration,

- Training,

- Data entry,

- Reporting,

- Back-up,

- Operations support,

- User support.

5.5 The laboratory should have documented policies and procedures for ensuring the integrity of the system, its software, firmware and any records produced and/or kept within the system. Integrity assurance policies and procedures must necessarily cover specification, procurement, acceptance, testing, access control, configuration control, protection from malicious intervention, for example viruses, where the possibility exists and other policies that are deemed necessary.

5.6 The system should be protected through the use of appropriate security measures. This might simply consist of physical access control to authorised users for stand-alone workstations or physical keyboard locking. Password control might be unnecessary in those circumstances and might even be unavailable on many computer systems. Appropriate security measures might also consist of double-shell security systems consisting of an outer shell protecting the system from unauthorised access and an inner shell protecting individual documents, files or groups of files from unauthorised access. The choice and solution depends on the possibilities available and the results of the risk analysis performed.

5.7 The laboratory should have documented procedures for making back-ups of all data and for the secure and safe storage of these. (See also 8.2).

5.8 The laboratory should have written procedures describing its policy on virus protection and how this is accomplished. See also 4.5.

6 Quality system, audit and review

6.1 Any deviation, planned or unplanned, from the written instructions defining the operation of the computer system fall within the framework of processing of anomalies and requires appropriate authorisation. The procedure followed for this authorisation must be sufficiently documented and recorded.

6.2 All parts of the quality system relating to the computer system of the laboratory should be included within the scope of the internal audit and management review.

7 Personnel

The laboratory should have documented procedures for the training and authorisation of personnel doing any work concerning the computer system. These procedures should include information and training in at least the following:

- All technical and administrative instructions and information necessary for the correct, safe and secure operation of the system;

- All technical and administrative procedures to be followed in case of system failure or any other anomalies that might come up during the day-to-day operation of the system;

- The extent and limitations of the responsibilities of each person qualified and authorised to work with the system, to maintain it or to modify it.

8 Accommodation and environment

8.1 All parts of the computer system including electronic storage media should be kept in an environment that ensures the safe and secure function of the system. Wherever necessary the laboratory should monitor and control the environmental

parameters that affect the safe and secure function of each part of the system including the area where records are kept on electronic media.

8.2 Electronic storage media should be kept in an environment that does not jeopardise the quality and accessibility of the data stored. The laboratory should specify the period during which accessibility is guaranteed. (See also 5.6).

9 Equipment and reference materials

9.1 The laboratory should establish documented policies and procedures for the installation, verification, maintenance and repairs of computer systems. Even though the standards for laboratory accreditation do not explicitly cover the topic of "purchase procedures", it would be good practice and would prevent problems during the lifetime of the system if the laboratory also establishes procedures for the specification and purchase of the system.

9.2 Description of the system

9.2.1 The laboratory should maintain a comprehensive description of the system. The degree of detail in which such a description is made should reflect the degree in which the computer or computer system influences the quality of the accredited work performed by the laboratory. When making such a description the laboratory should consider at least the following:

− A list of all the individual parts of the system uniquely identified. The manufacturer's identification of the individual parts, including hardware, software and firmware can be sufficient for this purpose.

- Records of current configuration, including hardware components, firmware versions and software installed, user written or otherwise. These may naturally consist solely of supplier delivery and installation records where no other changes are made.

- An overall description of the function and instructions for use of the system: hardware, software and firmware as appropriate.

- Where appropriate, a diagram showing the function of the data flow between the different parts of the system and the software employed.

- A textual or schematic description of the software incorporated in the system.

- A description of the data processing procedures in the system including formulae, algorithms, correction factors used, etc.

- An estimation of the measurement uncertainty introduced by the system to the final result.

9.2.2 The description of the system should be updated after any changes are incorporated, for example new version of the software, a change in function, a new auxiliary part, etc.

9.2.3 The current configuration of the system may be represented by a wide range of user controlled parameters. It is essential that these are recorded and available either electronically or otherwise. The present state shown by the system is not sufficient, as the purpose of such records is to show the state at the time of any

result obtained and to enable reconfiguration in the event of failure.

10 Measurement traceability and calibration of the computer or computer system

10.1 The acceptance test and initial verification of the system

10.1.1 The laboratory should have documented procedures to verify that the system performs in compliance with the requirements stated in its quality system documents and the requirements of the tests in question. The function of the system can be verified and documented through the use of one or more of the following procedures as might be relevant or any other relevant methods:

- By using software test tools whenever these are available;

- By simulating a test process through input of theoretical values into the computer unit of the system;

- By making measurements or tests on one or more objects with known outcome.

- By using certified test data sets where appropriate and available.

10.1.2 In the case of new equipment, these activities can be part of the acceptance testing procedures:

- All software incorporated in the system should be uniquely identified. The procedure for the verification of software should be part of the quality system of the laboratory. The verification procedure (function control, compilation, de-bugging, etc.) should be recorded for each individual verification performed.

10.2 Calibration of the system

The requirements on calibration are the same for all measurements performed by an accredited laboratory, independent of whether the measurement is made using a conventional instrument, a "black-box" or a computer system. However, it might not always be evident that a computer, computer system or a "black-box" has integrated measuring devices which require calibration and traceability. In the text that follows a description is given as to how the requirements on traceability can be achieved for computers and computer systems.

10.2.1 Computer systems for measurement and testing incorporate measurement units for measuring physical or other quantities. Therefore they should be treated in the same way as any other measuring instrument concerning the requirements on traceability. All quantities affecting the result of the test or measurement should be calibrated with documented traceability. This calibration should if possible be made by direct methods. If this is not possible the laboratory should develop procedures for achieving the same traceability through indirect methods.

10.2.2 In some cases the system, including integrated measurement devices, is treated as a black box. In such cases it may not be necessary or possible to analyse the measurement uncertainty contribution of each individual part and the total uncertainty should be estimated according to EAL-G23. In cases where the system is used for accredited calibration activities EAL-R2 applies.

10.2.3 In cases where it is necessary to separate a measurement device from the rest of the system a calibration should be made directly of the measurement unit in question. After each such measurement device has been calibrated it might be necessary to make a total verification of the system by using one or more of the procedures described in the previous section.

10.2.4 In cases where it is not possible to make a direct calibration of the individual measurement devices incorporated in the system, the laboratory should develop other (indirect) methods for calibrating the measurement units of the system so that full traceability is achieved. In this case it is particularly important to end the calibration activity by performing a verification procedure.

10.2.5 In cases where the system incorporates measurement units for which traceability to international standards is not possible to obtain, the traceability of measurements should be achieved through other internationally accepted means like the use of reference materials or reference objects. (See EAL guide G12).

10.2.6 For parts of the system where an estimation of the measurement uncertainty cannot be made through calibration procedures, the laboratory should have documented procedures for the evaluation of the measurement uncertainty introduced by each part and their contribution to the total measurement uncertainty.

10.2.7 Computer systems include such components as timers, including system clocks, and A/C-converters which might require calibration or checking where they contribute to measurement results.

10.3 Verification of the system after a change has been incorporated

10.3.1 A change is said to be incorporated in the system when one of the following activities or any other equivalent activity has taken place:

- Parts of the hardware of the system have been repaired;

- New hardware has been installed;

- A new version of the present software has been installed;

- New software has been installed;

- New auxiliary equipment has been installed;

- The system has had to go through other changes due to new requirements on the system;

- Changes to configuration parameters;Addition of or modification to software, including user-written routines, automation facilities, etc.

10.3.2 After any change in the system configuration relevant verification procedures should be performed.

10.4 Continuous maintenance of the system

10.4.1 There should be documented procedures for the maintenance of the computer system during its use. All maintenance activities, whether preventive or corrective, should be performed by authorised personnel. If the laboratory subcontracts these activities, it should make sure that the subcontracted activity meets the quality requirements of the laboratory.

10.4.2 The maintenance of the computer system should include periodic verification activities equivalent to one or more of the procedures for the initial verification of the system.

11 Calibration and test methods

11.1 All relevant documents, manuals, instructions and other procedures necessary for the use and maintenance of the system should be in a language readily understood by the relevant personnel.

11.2 The laboratory should have written procedures describing the tests to be performed using the computer system. The procedures should, besides a description of the test to be performed, contain at least the following information, unless this is made redundant by other documents:

- List of raw data to be recorded;

- Ways of data acquisition;

- Interpretation of errors and alarms produced by the software and procedures to be followed when they occur.

11.3 The laboratory should have policies and procedures laying out the method of acquiring and processing the data in such a way that relevant staff can follow the procedure consistently and accurately. This would naturally include the acquisition of raw data, all system settings necessary and instructions on initiating and controlling acquisition and processing of data. In many systems, configuration files hold necessary method-specific configuration information. Clearly, where this is the case, those files constitute part of the system configuration and must themselves be duly controlled in the same way as the software itself.

11.4 In estimating the measurement uncertainty for the accredited test and calibration activities the laboratory should also take into consideration any contributions from the computer system, for example rounding errors, quantization errors, etc.

12 Handling of calibration and test items

When computers and computer systems are used for testing and calibration, the laboratory should have documented procedures that ensure traceability between each individual test sample fed into the system and the result produced by the system. Special care should be taken when a group or batch of test items is fed into the system at the same time.

13 Records

This chapter is, by no means made redundant by guidance given in other places in the document. It complements the guidance given, by setting up the framework for the records to be kept from the quality assurance activities.

13.1 There should be records of:

- The purchasing specifications of the system;

- All calibration, verification and maintenance activities performed and all changes incorporated in the system;

- The results of all calibration and verification activities;

- Any system failures and regeneration;

- The hardware and software configuration details of the computer system at the time of each particular calibration or test, or at each stage of calibration or testing.

13.2 As a result of the installation procedure, records should be kept of at least the following:

- Unique identification of the system in all parts;

- The installation procedure;

- The verification procedure chosen;

- Data and other results from the installation and verification procedures;

- The integration of the system in the present computer system of the laboratory;

- Verifying that the installation is correct.

13.3 The software verification records should contain, at least:

- Unique identification of the software verified;

- Data and other results from the verification process;

- Signature and identity of the person(s) undertaking the verification and authorising its results.

13.4 Data should be recorded in such a way as to prevent modification after its final approval. If modification is allowed there should be procedures providing full traceability of the modification including its justification.

13.5 There may be cases where there are good reasons for reviewing previously approved results. It is important that raw data be retained untouched where possible and it is recommended that measures are taken to ensure continued integrity of raw data. It is also important to ensure that all relevant procedures and parameters used in producing a result from raw data are recorded as far as possible. There is no justification for modifying raw data and associated records.

13.6 All raw data as well as the necessary documentation for its interpretation and analysis must be recorded for a period of time defined by the laboratory and brought to the knowledge of its clients.

13.7 Whenever major changes are implemented in the system or new systems are installed, the laboratory should ensure that recorded and stored data remains accessible.

13.8 When changes are implemented in the system or new systems are installed, the laboratory should make sure that reports issued in the previous system can still be read and dispatched during the total period of storage as prescribed by the quality system.

13.9 Original observations, calculations and derived data, calibration records and final test reports stored by electronic means should be marked by a unique identification that makes them traceable to the test item, test and customer in question. If the data stored by electronic means is only part of the total record concerning a specific test, the records not kept electronically should be marked in such a way that there is traceability between all records related to a specific test. This traceability should be achieved in such a way that there is no doubt as to which test item, test and customer the records are related to.

13.10 If back-ups are used as the medium for retaining records, i e as archiving, or if they are used to restore a system to a previous state, i e to generate results, it is important that the procedure is in place and works. It should be mentioned that a laboratory is never going to be able to demonstrate a full restore from last back-up to satisfy an auditor as this would involve a full prior system back-up, shutdown and restore, followed by restoration of the current data.

13.11 Whenever records are stored electronically they must be retrievable.

13.12 Data entry

13.12.1 The integrity of data is most vulnerable at the moment of acquisition, whether this is done by manual means or by a computer system. The laboratory must ensure that:

− The person responsible for the direct entry of data is identified at the moment of acquisition;

- The device used for the transfer of data and the date of transmission is recorded.

13.12.2 Special care should be taken to protect electronically stored records from electromagnetic interference and damage. The parts of the system or the physical area where the records are kept should not be accessible by unauthorised persons and should meet all requirements of safety, security and confidence to the client.

14 Certificates and reports

14.1 Systems for electronic transmission of final reports must either convey, or make it possible to obtain independently, the information required in standard certificates of testing. Test reports generated and despatched by electronic means should carry a code or signature that uniquely identifies the person(s) accepting technical responsibility for the test report. It should also carry a unique code identifying the laboratory issuing the report.

14.2 The laboratory should have documented procedures for verifying the correctness of the electronic transfer to the customer and should if requested be able to dispatch the same report in hard copy . If the test report contains information or annexes that are not possible to transfer by electronic means, for example photographs, a paper version of the complete report together with the annexes should be sent to the customer. The laboratory should maintain all reasonable control over data transmission to ensure that data is transmitted to the correct receiver and without distortion.

14.3 Any corrections to a report produced by electronic means should be made according to the same principles as for reports produced on paper.