Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

22-Apr-2016

English - Or. English

ENVIRONMENT DIRECTORATE
JOINT MEETING OF THE CHEMICALS COMMITTEE AND THE WORKING PARTY ON CHEMICALS, PESTICIDES AND BIOTECHNOLOGY

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING
Number 17

Advisory Document of the Working Group on Good Laboratory Practice

Application of GLP Principles to Computerised Systems

JT03394591

Complete document available on OLIS in its original format

ENV/JM/MONO(2016)13 Unclassified

English - Or. English

OECD Environment, Health and Safety Publications

Series on Principles of Good Laboratory Practice and Compliance Monitoring

No. 17

Advisory Document of the Working Group on Good Laboratory Practice

Application of GLP Principles to Computerised Systems

Environment Directorate

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT

Paris 2016

ALSO PUBLISHED IN THE SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

- *No. 1, OECD Principles of Good Laboratory Practice (as revised in 1997)*
- *No. 2, Revised Guides for Compliance Monitoring Procedures for Good Laboratory Practice (1995)*
- *No. 3, Revised Guidance for the Conduct of Laboratory Inspections and Study Audits (1995)*
- *No. 4, Quality Assurance and GLP (as revised in 1999)*
- *No. 5, Compliance of Laboratory Suppliers with GLP Principles (as revised in 1999)*
- *No. 6, The Application of the GLP Principles to Field Studies (as revised in 1999)*
- *No. 7, The Application of the GLP Principles to Short-term Studies (as revised in 1999)*
- *No. 8, The Role and Responsibilities of the Study Director in GLP Studies (as revised in 1999)*
- *No. 9, Guidance for the Preparation of GLP Inspection Reports (1995)*
- *No. 10, The Application of the Principles of GLP to Computerised Systems (1995)*
- *No. 11, The Role and Responsibilities of the Sponsor in the Application of the principles of GLP (1998)*
- *No. 12, Requesting and Carrying Out Inspections and Study Audits in Another Country (2000)*
- *No. 13, The Application of the OECD Principles of GLP to the Organisation and Management of Multi-Site Studies (2002)*
- *No. 14, The Application of the Principles of GLP to in vitro studies (2004)*
- *No. 15, Establishment and Control of Archives that Operate in Compliance with the Principles of GLP (2007)*
- *No. 16, Guidance on the GLP Requirements for Peer Review of Histopathology (2014)*

ABOUT THE OECD

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation in which representatives of 34 industrialised countries in North and South America, Europe and the Asia and Pacific region, as well as the European Commission, meet to co-ordinate and harmonise policies, discuss issues of mutual concern, and work together to respond to international problems. Most of the OECD's work is carried out by more than 200 specialised committees and working groups composed of member country delegates. Observers from several countries with special status at the OECD, and from interested international organisations, attend many of the OECD's workshops and other meetings. Committees and working groups are served by the OECD Secretariat, located in Paris, France, which is organised into directorates and divisions.

The Environment, Health and Safety Division publishes free-of-charge documents in 11 different series: **Testing and Assessment; Good Laboratory Practice and Compliance Monitoring; Pesticides; Biocides; Risk Management; Harmonisation of Regulatory Oversight in Biotechnology; Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Registers; Emission Scenario Documents; and Safety of Manufactured Nanomaterials.** More information about the Environment, Health and Safety Programme and EHS publications is available on the OECD's World Wide Web site (www.oecd.org/ehs/).

This publication was developed in the IOMC context. The contents do not necessarily reflect the views or stated policies of individual IOMC Participating Organisations.

The Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) was established in 1995 following recommendations made by the 1992 UN Conference on Environment and Development to strengthen co-operation and increase international co-ordination in the field of chemical safety. The Participating Organisations are FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, World Bank and OECD. The purpose of the IOMC is to promote co-ordination of the policies and activities pursued by the Participating Organisations, jointly or separately, to achieve the sound management of chemicals in relation to human health and the environment.

OECD Environment Directorate,
Environment, Health and Safety Division
2 rue André-Pascal
75775 Paris Cedex 16
France

Fax: (33-1) 44 30 61 80

E-mail: ehscont@oecd.org

FOREWORD

The OECD Working Group on Good Laboratory Practice, at its 26th meeting in 2012, established a drafting group under the leadership of Austria's Federal Office for Safety in Health Care (Rd. Ronald BAUER) to update the 1995 OECD GLP Consensus Document number 10 - The Application of the Principles of GLP to Computerised Systems. The drafting group included representatives from Austria, Belgium, Ireland, Italy, Switzerland, the UK and the US EPA.

The following Advisory Document replaces the 1995 consensus document. It retains all of the key text from the original Consensus Document number 10, but includes new text to reflect the current state-of-the art in this field. This draft Advisory Document was posted on the GLP public web site on 17 September, 2014 and members of the public were invited to comment by 14 November 2014. This document reflects those comments.

This document is published under the responsibility of the Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology of the OECD.

TABLE OF CONTENTS

1. PREAMBLE

1. This document introduces a life cycle approach to the validation and operation of computerised systems. It emphasises risk assessment as the central element of a scalable, economic and effective validation process with a focus on data integrity. The intention of this document is to provide guidance that will allow test facilities to develop an adequate strategy for the validation and operation of any type of computerised system, regardless of its complexity, in a GLP environment.

1.1. Scope and definition of terms

2. Relevant terms are defined in the Glossary in Appendix 2.

1.1.1. Computerised System

3. This guidance applies to all types of computerised systems used in GLP regulated activities regardless of their complexity (ranging from simple devices like balances to more complex devices such as stand-alone PCs controlling lab-based instruments and complex systems like laboratory information management systems). The computerised system consists of hardware, software, and interfaces to its operating environment. Hardware consists of the physical components of the computerised system; it includes the computer unit itself and its peripheral components. Software is the program or programs that control the operation of the computerised system. All GLP Principles that apply to equipment therefore apply to both hardware and software. During the planning, conduct, reporting and archiving of studies, there may be several computerised systems in use for a variety of purposes. Such purposes might include the direct or indirect capturing of data from automated instruments, operation/control of automated equipment and the processing, reporting and storage of data. Consequently there should be appropriate procedures to control, maintain and operate computerised systems.

1.1.2. Validation

4. The demonstration that a computerised system is suitable throughout its life cycle for its intended purpose is of fundamental importance and is referred to as computerised systems validation. All computerised systems used for the generation, measurement, calculation, assessment, transfer, processing, storage or archiving of data intended for regulatory submission or to support regulatory decisions should be validated, and operated and maintained in ways that are compliant with the GLP Principles. The same requirement also applies to computerised systems used to produce other GLP-relevant data such as records of raw data, environmental conditions, personnel and training records, maintenance documentation, etc. The process a computerised system performs should be reliable and fit for purpose. The validation process must provide a high degree of assurance that a computerised system meets its pre-determined specifications. Validation should be undertaken by means of a formal validation plan and performed prior to operational use.

5. Validation of newly established computerised systems should be done prospectively. Depending on the size, criticality and novelty of the system, testing should be performed if possible in a dedicated validation environment before transfer into the laboratory environment. It must be ensured that the validation environment is equivalent to the laboratory environment for appropriate simulation. Appropriate change control should be applied throughout the system's life cycle including its retirement.

6. Retrospective validation is not permitted unless the scope of use has changed or an existing system has become GLP-relevant (e.g., the need for compliance with the GLP Principles was not foreseen or specified). Where this occurs there should be a documented justification prior to the use of the system in a GLP study. This should involve a retrospective evaluation to assess suitability that begins with gathering relevant historical records related to the computerised system. These records should be reviewed and a written summary should be produced. This retrospective summary should specify what evidence is available and what additional requirements must be tested during formal acceptance testing to achieve the validated status.

1.1.3. Qualification

7. Formal qualification rather than validation may be acceptable for Commercial Off-The-Shelf systems (COTS), automated equipment of low complexity or small systems. Due to its extensive use, validity of the incorporated software can be assumed in cases where no customisation is performed. Reference is made to respective guidance from the Good Manufacturing Practice (GMP) area, as e.g. Annex 15 of the EU *Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use*, regarding "Qualification and Validation."

8. Examples of low complexity COTS, automated equipment or small systems may be: analytical equipment such as electronic pipettes, balances, photometers and storage devices like refrigerators, freezers, etc.

9. Test facility management must decide and define criteria for when to apply computerised system validation and/or qualification approaches. A risk based approach should be applied to define critical process parameters and the actions used to monitor each process to ensure it remains in a state of control throughout the life cycle of the computerised system. Therefore it is expected that stringent calibration and maintenance measures are in place, along with the use of internal references or standards with strict pre-defined specifications. Application of statistical process control tools (e.g., control charts) are recommended and long term traceability of monitoring results is expected. Special focus and monitoring is expected with regard to the control of data flow where interfaces to other systems are established. Standard procedures shall be in place that clearly describe defined process and control steps.

10. Re-qualification activities should be performed based on pre-defined time periods taking into account identified risks. The qualification approach should be detailed in procedures.

11. Existing qualification plans and reports may be referenced when multiple examples of the same equipment are used within the test facility.

1.1.4. Life cycle

12. The validation approach should be risk-based and test facility management has the freedom to choose any appropriate life cycle model. It should ensure validation activities are defined and performed in a systematic way from conception, understanding the requirements, through development, release, operational use, to system retirement. All relevant phases of the life cycle should be documented and defined. This may include the purchase, specification, design, development and testing, implementation, operation and retirement of computerised systems. Life cycle activities should be scaled based on

documented risk assessment. Minimal activities may be required for simple processes like weighing on a stand-alone balance; more extensive activities might be required for complex systems like interfaced laboratory information management systems.

1.2. Risk management

13. Risk management should be applied throughout the life cycle of a computerised system taking into account the need to ensure data integrity and the quality of the study results. Risk management consists of risk identification, risk assessment, risk mitigation and risk control. Decisions on the extent of validation and data integrity controls should be based on a documented rationale and documented risk assessment. Risk management should link to other relevant procedures (e.g. configuration and change management, management processes for data, business risks, etc.).

14. Risk assessment should be used to develop an adequate validation strategy and to scale the validation efforts. The validation effort should be driven by the intended use of the system and potential risks to data quality and data integrity. The outcome of the risk assessment process should result in the design of appropriate validation activities for computerised systems or computerised system functionalities. The appropriate use of risk assessments is of paramount importance for an effective and efficient validation approach. If risk assessment outcomes are appropriately used they will provide test facility management with an adequate methodology to validate both simple laboratory systems as well as complex laboratory data management systems.

15. Risk assessment of computerised systems that are used both for GLP-studies and non-GLP studies should include any potential impact of non-GLP activities on GLP compliant activities. The same requirements for validation apply for such systems as for computerised systems that are used exclusively in GLP studies. There should be a clear differentiation of GLP data from non-GLP data.

1.3. Personnel, roles and responsibilities

16. The GLP Principles require that a test facility or a test site have appropriately qualified and experienced personnel and that there are documented task specific training programmes including both on-the-job training and, where appropriate, attendance at external training courses. Records of all such training should be maintained. The same provisions also apply for all personnel involved with computerised systems. Tasks and responsibilities of test facility management, quality assurance, study director and study personnel that use or maintain computerised systems should be defined and described.

17. To validate a system and to operate a validated system, there should be close cooperation between all relevant personnel if possible such as the test facility management, the study director, quality assurance personnel, IT personnel and validation personnel. All personnel should have appropriate qualifications and be provided with appropriate levels of access and defined responsibilities to carry out their assigned duties.

18. Personnel who validate, operate and maintain computerised systems are responsible for performing their activities in accordance with the GLP Principles and best practice guidance and standards (see "References" in Chapter 5 below).

19. During validation of computerised systems and the conduct of GLP studies, roles and responsibilities should be defined and controlled via system access privileges, training and general GLP requirements. Training records and system access authorisations of users should be available and demonstrate that personnel have sufficient knowledge and access rights to fulfill their respective roles in a GLP compliant manner.

20. Relevant contracts or service level agreements should detail GLP training requirements for global or corporate IT teams or for external and internal IT service providers who may work in accordance with quality management systems other than GLP.

21. *Roles and Responsibilities* are described in Appendix 1.

1.3.1. Test facility management

22. Test facility management has overall responsibility to ensure that the facilities, equipment, personnel and procedures are in place to achieve and maintain validated computerised systems.

23. This includes:

a) the responsibility to establish procedures to ensure that computerised systems are suitable for their intended purpose and are operated and maintained in accordance with the Principles of GLP;
b) the appointment and effective organisation of an adequate number of appropriately qualified and experienced staff; and
c) the obligation to ensure that the facilities, equipment and data handling procedures are of an adequate standard.

24. Test facility management should ensure that procedures required to achieve and maintain the validated status of computerised systems are understood and followed, and ensure that effective monitoring of compliance occurs.

25. Test facility management should designate personnel with specific responsibility for the development, validation, operation and maintenance of computerised systems. Such personnel should be suitably qualified, with relevant experience and appropriate training to perform their duties in accordance with the GLP Principles.

26. It is the overall responsibility of the local test facility management to ensure that computerised systems provided within a wider company are operated and maintained locally in accordance with the Principles of GLP. Written agreements between the local test facility management and the parent organisation should clearly assign responsibilities for validation and maintaining the validated status and GLP compliant operation of computerised systems. Test facility management can delegate responsibilities fully or partly at an individual system level or collectively to adequately trained personnel (e.g. the overall responsibility for GLP compliance of computerised systems to a system owner or for a specific computerised system to a validation director).

27. The test facility management should define roles and responsibilities for both validation activities and the routine operation of each computerised system regardless of its level of complexity. Potential conflicts of interest associated with roles and responsibilities should be considered to avoid risks to data integrity (e.g. analytical personnel should not be in control of the audit trail settings of the system they are working with).

1.3.2. Study Director

28. The study director is responsible for the overall conduct and GLP compliance of the studies. The study director has the responsibility to ensure that all computerised systems used in the studies are validated and used appropriately. The study director's responsibility for electronic data is the same as that for data recorded on paper (data should be attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available). Before the initiation of a GLP study, confirmation of the

validation status of all the computerised system(s) that will be used should be verified by the study director.

1.3.3. Quality assurance

29. Quality assurance personnel should be aware of GLP-relevant computerised systems at their test facility or test site. Quality assurance responsibilities for computerised systems should be defined by test facility management and described in written procedures. Quality assurance should be able to verify the valid use of computerised systems. The quality assurance program should include procedures and practices that verify if established standards are met for all phases of a system's life cycle. Tasks to verify standards in validation, operation and maintenance of computerised systems may be delegated to experts or specialist auditors (e.g. system administrators, system owners, external experts etc.). Quality assurance personnel should be provided with an appropriate level of training and access to allow them to inspect specific computer processes if needed (audit trail reviewing, data analysis techniques, etc.). During inspections of studies, quality assurance personnel should have direct read-only access to the data if it is only available within a computerised system.

30. Study directors and quality assurance personnel should have sufficient training to understand the relevant procedures in adequate use of GLP-relevant computerised systems.

1.4. Facility

31. Due consideration should be given to the physical location of computer hardware, peripheral components, communications equipment and electronic storage media. Extremes of temperature and humidity, dust, electromagnetic interference and proximity to high voltage cables should be avoided unless the equipment is specifically designed to operate under such conditions.

32. Consideration must also be given to the electrical supply for computer equipment and, where appropriate, back-up or uninterruptable supplies for computerised systems whose sudden failure would affect the results of a study. Adequate facilities should be provided for the secure retention of electronic storage media.

1.5. Inventory

33. An up-to-date listing (inventory) of all GLP-relevant computerised systems and their functionality should be maintained. The list should cover all GLP-relevant computerised systems, regardless of their complexity. Computerised systems used in GLP studies should be traceable from the study plan or relevant method to the inventory. The inventory should contain the validation status, make, model or version as relevant, and business process owner and IT system owner (persons who have responsibility or accountability for the system).

1.6. Supplier

34. When suppliers (e.g. third parties, vendors, internal IT departments, service providers including hosting service providers) are used to provide, install, configure, integrate, validate, maintain, modify decommission or retain a computerised system or for services such as data processing, data storage, archiving or cloud services, then written agreements (contracts) should exist between the test facility and the supplier. These agreements should include clear statements outlining the responsibilities of the supplier as well as clear statements about data ownership.

35. The competence and reliability of a supplier should be evaluated by test facility management. The need for, and extent of, vendor assessment should be based upon a risk assessment taking into account

the complexity of the computerised system and the criticality of the business process supported by the computerised system. The need for an audit should be based on a documented risk assessment. It is test facility management's responsibility to justify the requirement for and type of audit based on risk.

36. If the evaluation scope includes a technical as well as compliance focus, the involvement of specialist technical personnel as well as quality assurance personnel should be considered. Test facility management should be able to provide inspectors with information about the quality systems of suppliers depending on the services they are providing. Suppliers do not need to conform to GLP regulations, but must operate to a documented quality system verified as acceptable by test facility management with input from the quality assurance unit.

37. For vendor-supplied systems, it is likely that much of the documentation created during the development is retained at the vendor's site. If documentation is retained at the vendor's site, test facility management should ensure it is securely stored. This may require a formal contract between the vendor and the test facility. In this case, evidence of a formal assessment and/or vendor audits should be available at the test facility. Formal acceptance testing by the test facility of vendor-supplied systems is required.

38. Test facility management should define in written agreements the interfaces between its validation procedures and any activities provided by a supplier. Such interfaces should be applicable to the validation phase and to the operational phase. For example, any testing activities performed by a supplier should be evaluated by the test facility management.

39. Hosted services (e.g. platform, software, data storage, archiving, backup or processes as a service) should be treated like any other supplier service and require written agreements describing the roles and responsibilities of each party. It is the responsibility of test facility management to evaluate the relevant service and to estimate risks to data integrity and data availability. Test facility management should be aware of potential risks resulting from the uncontrolled use of hosted services.

40. A test facility may include the company's IT department as a part of its GLP facility. In such cases they must have a reporting line to test facility management.

1.7. Commercial Off-The-Shelf products (COTS)

41. A computerised system may fully or partially rely on COTS products. COTS products may be used without modification, with limited configuration, with heavy configuration or even customised coding. As with any other type of software, COTS products require appropriate validation depending on the risk and the complexity of any customisation. If an application (e.g. a spreadsheet) is not complex, it might be sufficient to verify functions against user requirement specifications.

42. User requirement specifications should be written for any application that is based on a COTS product. Documentation supplied with a Commercial Off-The-Shelf (COTS) product should be verified by test facility management to ensure it is able to fulfill user requirement specifications.

43. Spreadsheet templates for calculations using pre-defined formulas, self-written equations, or macros should be regarded as in-house developed applications. The validation requirements for these are described in sections 2 and 3 and will depend on risk and complexity. The underlying COTS product will require an appropriate form of qualification and documentation. Qualification of the underlying COTS product alone is not sufficient.

1.8. Change and configuration control

44. Any changes to a computerised system should be made in a controlled manner and in accordance with written change control procedures. Change control procedures should cover the validation phase, the operational phase (including archiving) and the phase in which the system is retired. Test facility management should define roles and responsibilities of those involved with change control activities. Decisions on change control requirements should be risk based and will depend on the complexity and criticality of the change to data integrity or the business processes supported by the computerised system. Risk assessment used in change control can utilise software categorisation as described in current ISPE[1] GAMP[2] guidance.

45. Change control should cover any item that undergoes review, approval and testing and that is relevant for a defined configuration of a computerised system. It should ensure that a system's configuration is accurately described and documented at all times. Study specific activities (e.g. data capturing, data calculation, etc.) should be traceable to a specific configuration of the computerised systems if the configuration is relevant for the results. Change control should be interfaced with risk assessment, testing, release and adequate documentation procedures.

1.9. Documentation requirements

46. Documentation requirements for computerised systems should be included in the quality management system and should cover all GLP-relevant computerised systems. The depth of documentation necessary will vary dependent on the complexity and validation strategy of the computerised system. For each computerised system there should be documentation typically covering:

a) the name and version of the computerised system's software or identification code and a detailed and clear description of the purpose of the computerised system;
b) the hardware on which the software operates;
c) the operating system and other system software (e.g., tools) used in conjunction with the computerised system;
d) the computerised system's programming language(s) and/or data base tools used where appropriate only;
e) the major functions performed by the computerised system;
f) an overview of the type and flow of data associated with the computerised system;
g) file structures, error and alarm messages associated with the use of the computerised system;
h) the computerised system's software components with version numbers; and
i) configuration and communication links among modules of the computerised system and to equipment and other systems.

47. The use of computerised systems should be documented adequately. Such documentation typically covers, but is not limited to:

a) procedures for the operation of computerised systems (hardware and software) and the responsibilities of personnel involved;
b) procedures for security measures to detect and prevent unauthorised access or changes to data;
c) change control procedures describing processes for authorisation, testing and documentation of changes to equipment (hardware and software);

[1] ISPE - International Society for Pharmaceutical Engineering
[2] GAMP - Good Automated Manufacturing Practice

d) procedures for the periodic evaluation for correct functioning of the complete system or its component parts and the recording of these tests;
e) procedures covering routine preventative maintenance and fault repair (these procedures should clearly detail the roles and responsibilities of personnel involved. For COTS systems, the use of a vendor's own policies and procedures for performing the work where appropriate is acceptable. This should be detailed in a written service level agreement);
f) procedures for software development, acceptance testing, and other relevant testing and the recording of all testing;
g) back-up and business continuity procedures;
h) procedures for the archiving and "retrieval" of all electronic data, software versions and documentation of computer configuration and evidence of all activities;
i) procedures for the monitoring and auditing of computerised systems and evidence of all activities; and
j) procedures and authorisation for system retirement.

48. Further management and validation procedures should be described if relevant and may comprise but not be limited to: acquisition; risk management; service management; validation planning; requirement specification; design specification; installation; system release; traceability; incident management; configuration management; record management; staffing; roles and responsibilities of personnel and document management.

49. Records and procedures should be available that describe in sufficient detail validation and use of the computerised system. Such records may comprise but are not limited to: risk assessment; supplier assessment; service level agreements; requirement specifications; testing; release; personnel and user training; descriptions of incidents and changes; configuration and operation.

50. The complete documentation of validation and operation of a computerised system should be available as long as study data generated with the system have to be archived according to applicable regulations.

2. PROJECT PHASE

2.1. Validation

51. Computerised systems should be designed and demonstrated to be fit for purpose in a GLP environment and introduced in a pre-planned manner. The validation of a computerised system, its documentation and reports should cover the relevant steps of the life cycle, as defined by test facility management based on the complexity and intended use of a system. The validation effort may be scaled and adapted to the type of system justified by documented risk assessment. Test facility management may rely on best practice guidance when scaling the validation effort. Test facility management should be able to justify the life cycle, the strategy, validation standards, protocols, acceptance criteria, procedures, records and corresponding deliverables based on a risk assessment. For example, test facility management`s validation deliverables may be limited to user requirement specifications, a validation plan, user acceptance testing and a validation report if it can be justified by risk assessment.

52. There should be evidence that the system was adequately tested for conformance with the acceptance criteria set by the test facility prior to being put into routine use. Formal acceptance testing requires the conduct of tests following a pre-defined plan and retention of documented evidence of all testing procedures, test data, test results, a formal summary of testing and a record of formal acceptance.

2.2. Change control during validation phase

53. A change control and deviation management process should be in place from the start of the validation process. If change control and deviation records are not considered relevant it should be justified by test facility management based on a risk assessment (e.g. a simplified validation approach of a less complex [i.e. simple] system).

54. Change control during development and validation of a system should be clearly distinguished from change control during the operation of the system. Validation documentation should include change control records (if applicable) and reports of all deviations observed during the validation process.

2.3. System description

55. A system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software prerequisites, and security measures should be available. An up-to-date system description should be maintained throughout the life cycle of the system as described in chapter 1.9. For simple systems with low complexity, a less complex description would be acceptable.

2.4. User requirement specifications

56. User requirement specifications are of paramount importance for all validation activities and should be generated for all GLP-relevant computerised systems regardless of the system's complexity. User requirement specifications should describe the functions of a system and should be based on a documented business process for the system, and the applicable regulatory requirements. An initial validation risk assessment should be based upon an understanding of the business processes, user requirement specifications and regulatory requirements.

57. User requirement specifications should cover all GLP-relevant functions of a system and should be used in the risk assessment to identify critical functions and appropriate testing activities. Depending on a system's complexity, user requirement specifications should be traceable to any further specification documents, if applicable, and test documentation generated throughout the life cycle.

58. If a provided system (purchased or hosted by a supplier) contains more functions than needed, only the GLP-relevant functions need to be tested. Validation should also include functions that may be used in non-GLP studies and that might interfere with the use of the computerised system in GLP studies. The other functions and/or functionalities that are out of scope (i.e. not intended to be used) should be identified but do not require testing.

2.5. Quality Management system and support procedures

59. Both the development of a computerised system as well as the validation process should be governed by a quality management system. There should be adequate documentation that a system was developed in a controlled manner and preferably according to recognised quality and technical standards (e.g. ISO 9001). If a system is developed by a vendor, it is the responsibility of test facility management to evaluate the vendor's system development quality management system. The test facility management should rely on risk assessment when defining the evaluation strategy.

2.6. Customised systems[3]

60. Customised systems are developed for a specific use by a particular test facility (e.g. GLP study specific data capturing systems, spreadsheet templates with formulas or macros, queries, statistical applications or data evaluation systems, etc.). Such computerised systems may also be configured or coded specifically for one or more GLP studies. As no experience from previous or parallel use is available, customised systems bear the highest intrinsic risk. There should be a process in place for the validation of customised computerised systems that ensure the formal assessment and reporting of quality and performance measures for all the life cycle stages of the system.

61. A written agreement between the supplier of the customised system and test facility management describing roles and responsibilities relevant to the system and its validation is necessary. The validation effort of the test facility management should consider all quality relevant activities of the supplier even at the supplier's business location. Any outsourced activities or in-house supplier activities should be part of the computerised system's life cycle.

62. If a hosted application is a custom coded or configured application, the system must be addressed both as a customised and a vendor-supplied system.

2.7. Testing

63. Testing (e.g. installation testing, user acceptance testing) should be carried out to ensure that a system meets predefined requirements. It is test facility management's responsibility to understand the need for testing and to ensure the completeness of the tests and test documentation. Testing should be based upon business process knowledge and intended use of the system. Procedures should describe how tests are conducted and clearly define roles and responsibilities and documentation requirements. It is the test facility management's responsibility to decide on the depth and breadth of the testing guided by risk assessment. Test facility management should ensure that all systems, including COTS systems, are tested and evaluated. A supplier's testing activity and documentation may assist the test facility management in its validation efforts and may supplement or replace test facility testing. Test facility management should retain evidence of testing regardless of whether the testing is done by the test facility or by a supplier demonstrating appropriate test methods and test scenarios have been employed. In particular, system (process) parameter limits, data limits and error handling should be considered.

64. The test facility management should consider a method specific user acceptance testing to demonstrate that the system is fit for performing a specific GLP study (e.g. prove the suitability of a system performing a typical analytical determination including calibration, measurements, calculations and data transfer to a LIMS).

65. An interface to change control procedures should exist. When testing leads to system changes these should be managed via change control. Evidence of adequate testing could be provided by maintaining records of internal testing results, or records of vendor auditing.

2.8. Data migration

66. Data migration may occur in the course of a GLP study or after a study has been finalised. Data migration should be part of the test facility management's validation scope if GLP-relevant data is affected

[3] Source code of customised systems (or all software of the computerised system) in some OECD member countries should be retrievable by the test facility management to provide the monitoring authority access to the software code. This can be done by archiving a digital copy of the source code, escrow arrangements, or written agreements.

regardless of the status of any GLP study project. If study records are archived in an electronic system, data migration may become relevant.

67. Where electronic data are transferred from one system to another, the process must be documented. It is test facility management's responsibility to ensure and demonstrating that data are not altered during the migration process. Conversion of data to a different format should be considered as data migration (e.g. from a proprietary data format to PDF). Where data are transferred to another medium, data must be verified as an exact copy prior to any destruction of the original data.

68. Data migration efforts may vary greatly in complexity and risks. Examples include:

a) version upgrades;
b) data conversions (from one database to another; to another data format; software upgrade related change of format);
c) same system migration (moving application; data from one server to another); and
d) migration from a source to a target system.

69. Migrated data should remain usable and should retain its content and meaning. The value and/or meaning of and links between a system audit trail and electronic signatures should be ensured in a migration process. It is the test facility management's responsibility to maintain the link between the readable audit trail or electronic signatures and the audited data.

2.9. Exchange of data

70. Communications related to computerised systems broadly fall into two categories: between computers or between computers and peripheral components. GLP-relevant data may be transported automatically, uni-directionally or bi-directionally, from one system to another system (e.g. from a remote data capturing system to a central data base, from spreadsheets to a LIMS, from a chromatography data management system to a LIMS, or from a spreadsheet to a statistics software application). All communication links are potential sources of error and may result in the loss or corruption of data. Appropriate controls of interfaces for security and system integrity must be adequately addressed during development, validation, operation and maintenance. Electronic data exchange between systems should include appropriate built-in checks for the correct and secure entry and processing of data. Network infrastructure should be qualified. However, this requirement is not meant to request validation of standard communication infrastructure and its procedures (e.g. the basic communication language of the internet TCP/IP [Transmission Control Protocol / Internet Protocol]).

3. OPERATIONAL PHASE

71. All computerised systems should be operated and maintained in a manner which ensures the continuity of the validated state.

3.1. Accuracy checks

72. Test facility management should be aware of all GLP-relevant data entered manually into electronic systems. It is test facility management's responsibility to adequately control any electronic data entry system regardless of its complexity. Risk assessment should be applied to identify the potential for erroneous data entry and to evaluate the criticality and consequences of erroneously or incorrectly entered data. Risk mitigation strategies should be described and implemented. This may result in the need for additional manual and/or electronic checks for the accuracy of entered data by a second operator or electronic system. When used, automated checks on data entry should be included in the validation of a computerised system (e.g. automatically applied validation scripts during manual data entry), the depth of validation efforts should be scaled based on risk assessment. The use of invalidated data entry systems should be excluded (e.g. uncontrolled use of spreadsheets). If manual control procedures are applied for manual data entry, the procedure should be assured by adequate documentation which will facilitate reconstruction of activities.

3.2 Data and storage of data

73. When data (raw data, derived data or metadata) are stored electronically, requirements for back-up and archiving purposes should be defined. Back-up of all relevant data should be carried out to allow recovery following failure which compromises the integrity of the system.

74. Stored data should be secured by both physical and electronic means against loss, damage and/or alteration. Stored data should be verified for restorability, accessibility, readability and accuracy. Verification procedures of stored data should be risk based. Access to stored data should be ensured throughout the retention period.

75. Hardware and software system changes must allow continued access to, and retention of, the data without any risk to data integrity. When a system or software is updated, it must be possible to read data stored by the previous version or other methods must be available to read the old data. Supporting information (e.g. maintenance logs, calibration records, configuration etc.) which is necessary to verify the validity of raw data or to reconstruct a whole study or parts of it should be backed-up and retained in the archives. Software should be retained in the archive if necessary to read or reconstruct data.

76. Regarding electronic records, test facility management should have:

a) identified any study relevant electronic records (e.g. raw data, derived data). It is necessary that raw data are identified for each computerised system no matter how raw data are associated with it (e.g. by storage on an electronic storage medium, by computer or instrument printouts etc.);
b) assessed the criticality of the electronic records for the quality of study results;
c) assessed potential risks to the electronic records;

d) established risk mitigation procedures; and
e) monitored the effectiveness of risk mitigation throughout the life cycle.

77. Regarding procedures, the test facility management should describe how electronic records are stored, how record integrity is protected and how readability of records is maintained. For any GLP-relevant time period, this includes, but may not be limited to:

a) physical access control to electronic storage media (e.g. measures for controlling and monitoring access of personnel to server rooms, etc.);
b) logical (electronic) access control to stored records (e.g. authorisation concepts for computerised systems as part of computerised system validation which defines roles and privileges in any GLP-relevant computerised system);
c) physical protection of storage media against loss or destruction (e.g. fire, humidity, destructive electrical faults or anomalies, theft, etc.);
d) protection of stored electronic records against loss and alteration (e.g. validation of back-up procedures including the verification of back-up data and proper storage of back-up data; application of audit trail systems); and
e) ensuring accessibility and readability of electronic records by providing an adequate physical environment as well as software environment.

78. Data storage should be considered for each computerised system used to perform GLP studies during the study phase and archiving period. It is not necessary to include the evaluation in the study documentation. However, test facility management should have a policy to explain how data are stored and how storage requirements are satisfied. This information should be part of the system validation documentation set. If the test facility hands over the electronic study data to a sponsor, the responsibility for the data transfers to the sponsor.

3.3. Printouts

79. If data are printed to represent raw data, all electronic data including derived data as well as metadata and (information about data changes if such changes are necessary to maintain the correct content and meaning of the data) should be printed. Alternatively all electronic records should be verifiable on screen in human-readable format and retained. This includes all information about changes made to records, if such changes are relevant for the correct content and meaning.

3.4. Audit trails

80. An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point. Audit trails need to be available and convertible to a human readable form. Depending on the system, log files may be considered (or may be considered in addition, to an audit trailing system) to meet this requirement. Any change to electronic records must not obscure the original entry and be time and date stamped and traceable to the person who made the change.

81. Audit trail for a computerised system should be enabled, appropriately configured and reflect the roles and responsibilities of study personnel. The ability to make modifications to the audit trail settings should be restricted to authorised personnel. Any personnel involved in a study (e.g. study directors, heads of analytical departments, analysts, etc.) should not be authorised to change audit trail settings.

82. A system should be in place that can ensures a risk based review of the audit trail functions, its settings and the recorded information. The test facility management may consider, but should not be limited to, individual events (e.g. user behavior, suspected data integrity issues) to review the audit trail records. Completeness and suitability of the audit trail functions and settings may be considered. GLP quality assurance personnel should be involved. A review of the audit trail functions should be based upon an understanding of the use of the system, the ability to modify the record and the controls preventing malicious alterations of the records.

83. The system should be able to highlight alterations made to previously entered data both on the screen and in any printed copies. The original and modified entries should be retained by the system. Audit trails may exist in some systems as a record of changes supplemental to the view to the data (on screen or printed). The original data should be stored together with the modified data. For example, any re-integrated chromatogram modified for the purpose of recalculation should be marked irrevocably.

3.5. Change management and configuration management

84. Test facility management should have appropriate procedures for configuration management and change management in the operational phase. Both change and configuration management should be applied to hardware and software. Change control measures should ensure that changes to the configuration of the computerised system that may affect the validation status are introduced in a controlled manner. A change should be traceable to appropriate change and configuration control records. Procedures should describe the method of evaluation used to determine the extent of retesting necessary to maintain the validated status of the system.

85. Change control procedures should clearly define roles and responsibilities for accessing and approving changes and detail procedures for assessing the change. Irrespective of the origin of the change (supplier or in-house developed system), appropriate information needs to be provided as part of the change control process. Change control procedures should ensure data integrity.

86. The configuration of a computerised system should be known at any point during its life cycle, from the initial steps of development through to retirement. The documented compliance of an analytical instrument's configuration with the provisions of method validation is required to demonstrate the adequate use of a computerised system in a GLP study – regardless of its complexity. Any GLP study result should be traceable to the relevant and validated system configuration to allow the verification of settings as provided by the study plan or the relevant method.

87. Changes may be required in response to incidents or to facility/study specific purposes. After modification or repair, the validation status of the system should be verified and documented.

88. Modifications implemented by routine automation (e.g. virus protection or operating system patches) should be part of formal change control or configuration management. The absence of change management for a computerised system should be justified and based on risk assessment.

3.6. Periodic review

89. Computerised systems should be periodically reviewed to confirm that they remain in a validated state, are compliant with GLP and continue to meet stated performance criteria (e.g. reliability, responsiveness, capacity etc.). The review should include, where appropriate, the current range of functionality, deviation records, incidents, upgrade history, performance, reliability and security that may have affected the validation status of the system. The frequency and depth of the periodic review should be determined based on a risk assessment considering complexity and GLP criticality. The periodic review should take into account any reported unexpected event that may have affected the validation status of a

system. The suitability of the review activities and the involvement of specialist personnel as well as GLP-relevant personnel (e.g. test facility management, quality assurance, IT support personnel, supplier etc.) should be justified. Responsibilities of personnel involved in periodic reviews of the validation status of computerised systems should be defined. The need for an interaction between the periodic review activities and the incident reporting system may be considered depending on a risk assessment. Results of periodic review activities and, when applicable, remedial actions should be documented.

90. Computerised systems of less criticality and less complexity may be excluded from the review if the exclusion is justified based on risk. A periodic review may be unnecessary when major (re-)validation activities have recently occurred and could therefore be postponed. If no unexpected events that may have affected the validated status were reported, automated COTS systems may be excluded from the review. A periodic user review should be done when required (e.g. in the event of organisational changes) or at least yearly as persons and access roles may change. The user review should also be done for COTS.

3.7. Physical, logical security and data integrity

91. Documented security procedures authorised by test facility management should be in place for the protection of hardware, software and data from corruption or unauthorised modification, or loss. Appropriate physical and/or logical controls should be implemented depending on the complexity and criticality of a system and the requirements of the organisation in which the system is operated.

92. Suitable control methods for preventing unauthorised physical access to the system (e.g. computer hardware, communications equipment, peripheral components and electronic storage media) may include the use of keys, pass cards, personal codes with passwords, biometrics, or restricted access to specific computer equipment (e.g. data storage areas, interfaces, computers, server rooms, etc.). Creation, change, and cancellation of access authorisations should be recorded. Authorisation records should be periodically reviewed based upon the criticality of the process supported by the computerised system and in case of relevant organisational changes in the test facility.

93. As maintaining data integrity is a primary objective of the GLP Principles, test facility management should ensure that personnel are aware of the importance of data security, the procedures and system features that are available to provide appropriate security and the consequences of security breaches. Such system features could include routine surveillance of system access, the implementation of file verification routines and exception and/or trend reporting.

94. For equipment not held within specific “computer rooms” (e.g. personal computers and terminals), there should be access controls to the area where the hardware is located (e.g. access control to a building, a laboratory area, or a specific room). Where such equipment is located remotely (e.g. portable components and modem links) additional measures may be taken that should be justified and risk based (e.g. cryptographic control).

95. It is essential that only qualified and approved versions of software are in use. Any introduction of data or software from external sources should be controlled. These controls may be provided by the computer operating system, by specific security routines, by routines embedded into the applications or by combinations of the above. Systems for data and for document storage should be designed to record the date, time and identity of operators entering, changing, confirming or deleting data.

96. The potential for corruption of data by a malignant code or other agents should be addressed if considered necessary. Security measures should be taken to ensure data integrity in the event of both short term and long term system failure.

97. An appropriate and well maintained authorisation policy should specify logical access rights to domains, computers, applications and data. User privileges should be defined for operating systems and applications, and should be adapted as required by the organisation of the test facility and in combination with the requirements of a particular GLP study. Roles and responsibilities of personnel granting user privileges should be defined.

98. User privileges within a computerised system should not interfere with the requirements for data integrity. The activities of any GLP study personnel should be traceable to the user privileges and activities within all relevant computerised systems and should be reflected in user privilege control documents. Administrator rights should not be given to persons with a potential interest in the data (e.g. the laboratory role 'analyst' is not compatible with the system role 'administrator' in a chromatography data management system). A user should not have a second role in a particular system that could interfere with the requirements for data integrity.

3.8. Incident Management

99. During the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken. The study director, test facility management, quality assurance and, if appropriate, the sponsor should be informed about incidents requiring remedial action. The study director is responsible for defining the criticality of incidents and for assessing the impact on the study. The root cause of an incident requiring remedial action should be identified and should form the basis of corrective and preventive actions. The priority for corrective and preventative actions should be determined. It should be possible to trace all incidents requiring remedial action reported for a computerised system to the affected GLP studies and vice versa.

100. Incident records should be maintained with the system documentation and periodically archived. Incident records should be archived and stored with the system relevant (validation) documentation as incident reports are needed for monitoring and periodic review. Test facility management should have incident management interfaced or integrated with change management, configuration management, periodic review and training. Incident review should be part of a periodic system evaluation.

3.9. Electronic signature

101. Electronic records may be signed electronically by applying an electronic signature.

102. Electronic signatures are expected to:

a) have the same legal consequences as a hand-written signature at least within the boundaries of the test facility;
b) be permanently linked to their respective record(s);
c) include the time and date that they were applied; and
d) allow the identification of the signatory and the meaning of the signature.

103. An electronic signature function of a computerised system should be addressed in the requirements for the system and validated and described in the system procedures. The test facility management should have identified those records which require a hand-written or an electronic signature. It is test facility management’s decision to rely on an electronic signature function if other means are possible (e.g. printing and signing by hand). The applied procedure should be described adequately.

104. Test facility management should ensure the establishment of an electronic signature policy in order to ensure the adequate use and maintenance of electronic signature functions of a computerised system. Personnel authorised to sign electronically should be clearly identified by name and bound by

name to the electronic signature policy. A person's role in a GLP study should be reflected by the meaning of the corresponding electronic signature applied by a study relevant computerised system and should be traceable to the system's authorisation policy. It might be necessary to adapt a computerised system's authorisation concept to study specific requirements.

105. Test facility management should ensure that the electronic signature is equivalent to the handwritten signature and its authenticity is undisputable at least within the boundaries of the test facility or test site. Password re-entry should be considered as a minimum requirement for an electronic signature. The actuation of a function key by a person logged into a system should not be considered as an electronic signature.

106. Metadata which are associated with the electronically signed record should be clearly identified (e.g. method settings and system configuration if relevant for the electronically signed analytical result etc.). The computerised system's signature function should ensure the timeliness of the linkage between the electronically signed record and the supporting metadata. It should not be possible for the user to change an applied electronic signature nor the link to the associated metadata. If a change to an electronically signed record or the supporting metadata occurs it should be explained, (electronically) signed and dated by the person responsible for the change. The impact of the change to an electronically signed record or the supporting metadata on the electronic signature should be evaluated as the change invalidates the electronic signature.

107. Test facility management may apply a "paper-based" procedure to sign records that are printed from the electronic system. It should be noted that paper printouts of an electronic record may not contain all of the information that is necessary to fully reconstruct the activities or provide the full meaning of the data. Certain supporting metadata relevant for the printed/signed record may be kept electronically in a hybrid solution. The use of such a hybrid system should be fully explained in facility procedures and justified via risk assessment. Based upon a risk assessment, printing has to be done on a clear understanding of the process and the information that will not be captured in the printout. The hybrid solution should be described clearly to identify all additional electronic records or supporting metadata which are represented by the printed and signed version of a record. An appropriate system for version control should ensure the timeliness of the linkage between the printed/signed record and the electronically maintained records. Access to modified or superseded records for traceability of changes and documentation of invalid results should be possible. However those records should be excluded from routine use. If a complete set of electronic records and its printed analogue are maintained in parallel, the test facility management should specify the regulated record type in order to apply the appropriate control procedure (e.g. if the complete set of information of an analytical system is printed and maintained electronically in parallel it should be define which set of information is the regulated one).

3.10. Data approval

108. If a procedure includes an electronic data approval process, the data approval functionality should be included as part of the system validation. The approval process should be described in facility procedures and be performed electronically within the system.

3.11. Archiving

109. With regards to archiving, this advisory document supplements OECD GLP Advisory Document Number 15 "Establishment and Control of Archives that Operate in Compliance with the Principles of GLP".

110. Any GLP-relevant data may be archived electronically. The GLP Principles for archiving must be applied consistently to electronic and non-electronic data. It is therefore important that electronic data is stored with the same levels of access control, indexing and expedient “retrieval” as non-electronic data.

111. Viewing electronic records without the possibility of alteration or deletion of the archived electronic records or replicating within a computerised system or to another computerised system does not constitute “retrieval” of records. Only when the possibility of alteration or deletion of the archived record exists, should that be considered access, withdrawal, “retrieval”, or removal of records and materials. The archivist should be able to control the assignment of "view only" access to archived electronic data in order to verify that the requirements for archived data are met.

112. Electronic data should be accessible and readable, and its integrity maintained, during the archiving period. If a hybrid solution is chosen (i.e. “paper-based” data and electronic data maintained in parallel) the test facility management should specify the regulated records for relevance in archiving.

113. Electronic archiving should be regarded as an independent procedure which should be validated appropriately. A risk assessment should be applied when designing and validating the archiving procedure. Relevant hosting systems and data formats should be evaluated regarding accessibility, readability and influences on data integrity during the archiving period. Consideration may have to be given to archiving electronic data in an open format that is independent from proprietary file format e.g. from an instrument manufacturer. Where data conversion is needed, the requirements from section 2.8 apply. The archivist, who holds sole responsibility, may delegate tasks during the management of electronic data to qualified personnel or automated processes (e.g. access control). For roles and responsibilities in the archiving process refer to OECD GLP Advisory Document Number 15.

114. Procedures have to be implemented to ensure that the long-term integrity of data stored electronically is not compromised. If data media, data formats, hardware or software of archiving systems (not the data collection systems) change during the archiving period, the test facility management should ensure that there is no negative influence on the accessibility, readability and integrity of the archived data. The continuing ability to retrieve the data should be ensured and tested. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring continued readability of the data should be established. This may, for example, include producing hard copy printouts or converting data to a different format or transferring data to another system. If migration of data including conversion to a different data format or printing is relevant, the requirements of this guidance for data migration should be met. Risk assessment, change control, configuration management and testing regime should be considered as relevant standard procedures when changes in the archiving system are required. As content and meaning of any electronic data should be preserved during the archiving period, the complete information package should be identified and archived (e.g. raw data, meta-data necessary to understand correctly the meaning of a record or to reconstruct its source, electronic signatures, audit trails, etc.).

115. If an electronically signed record is archived electronically, its integrity should be ensured for the relevant time period. The verification of the integrity of the signed record, the supporting metadata and the electronic signature should be possible and subjected to evaluation within the archiving period. The periodicity of the evaluation should be justified by the test facility management based on risk assessment.

116. In the study report, the study director should identify all GLP-relevant electronic data which are subject to electronic archiving and the location of the electronic archive.

117. Any data held in support of relevant computerised systems, such as source code, development, validation, operation, maintenance and monitoring records, should be held for at least as long as study records associated with these systems.

118. No electronically stored data should be destroyed without test facility management and, where applicable, the sponsor's authorisation and relevant documentation.

3.12 Business continuity and disaster recovery

119. Provisions should be made to ensure the continuity of support for computerised systems which are used for GLP-relevant processes in the event of a system breakdown (e.g. a manual data entry or alternative computerised system). The time required to bring the alternative arrangements into use should be based on a risk assessment which should be appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

120. Procedures should be in place describing the measures to be taken in the event of partial or total failure of a computerised system. Measures may range from planned hardware redundancy to transition back to an alternative system. All contingency plans need to be well documented and validated and they should ensure continued data integrity and that the study is not compromised in any way. GLP personnel should be aware of such contingency plans.

121. Procedures for the recovery of a computerised system should depend on the criticality of the system, but it is essential that original or back-up copies of all software in the version relevant for the validated computerised system are maintained, escrowed, or available by service level agreement. If recovery procedures entail changes to hardware or software, the validation requirements of this guidance apply.

122. Where an alternative data capturing procedure is applied, if the manually recorded data is subsequently entered into the computer it should be clearly identified as such. The data entry process should be validated and there should be a statement that entered data is equivalent to the manually recorded raw data. The manually recorded raw data should be retained as the original record and archived as such. The full retention period of the manually recorded raw data is required. Alternative back-up procedures should serve to minimise the risk of any data loss and ensure that these alternative records are retained.

4. RETIREMENT PHASE

123. The system retirement should be considered as a system life cycle phase. It should be planned, risk based and documented. If migration or archiving of GLP-relevant data is necessary, risks to data should be excluded and the requirements of this guideline apply.

5. REFERENCES

"Good Practices for Computerised Systems in Regulated GxP Environments" [effective 25.09.2007] PIC/S PI 11-3

"Computerised Systems used in Nonclinical Safety Assessment: Current Concepts in Validation and Compliance" [published 2008, DIA, Red Apple II]."

"GAMP 5 - A Risk Based Approach to Compliant GxP Computerised Systems" ISPE Good Automated Manufacturing Practice © ISPE 2007

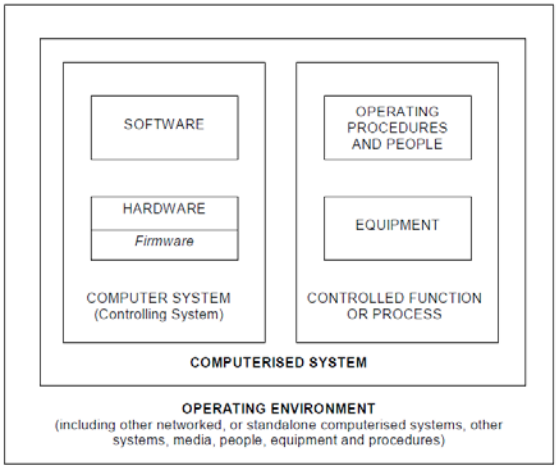
"Establishment and Control of Archives that Operate in Compliance with the Principles of GLP", [ENV/JM/MONO(2007)10], OECD GLP Advisory Document Number 15.

The rules governing medicinal products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Annex 15 to the EU Guide of GMP "Qualification and Validation" October 2015.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Business Process Owner	The individual or organisation responsible for providing the resources for a business process (e.g. a preclinical trial)
IT Personnel	Personnel involved in the purchase, installation and maintenance of a computerised system. Responsibility includes, for example, operating and maintaining the hardware and software, conducting backups, resolving problems, etc.
Personnel	Any person involved in validation, operation or support of a computerised system.
Quality Assurance	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.8.)
Sponsor	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.5.)
Study Director	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.6.)
Supplier	Third parties, vendors, internal IT departments, service providers including hosted service providers, etc.
System Owner / IT Owner	The individual who is responsible for the availability, support and maintenance of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerised system is supported and maintained in accordance with applicable procedures. The System Owner acts on behalf of the test facility management. Global IT systems may have a global system owner and local system owners to manage local implementation (see GAMP 5).
Test facility management	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.3.)
User	The personnel operating the computerised system in a GLP study.
Validation Director	A delegated person responsible for a validation project.

Appendix 2: Glossary

Term	Definition
Acceptance Criteria	The documented criteria that should be met to successfully complete a test phase or to meet delivery requirements.
Acceptance testing	Formal testing of a computerised system in its anticipated operating environment to determine whether all acceptance criteria of the test facility have been met and whether the system is acceptable for operational use.
Authorisation concept	An authorisation concept is a formal procedure to define and control access rights to and privileges in a computerized system.
Back-up	Provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment after a system failure or disaster.
Change Control	Ongoing evaluation and documentation of system operations and changes to determine whether a validation process is necessary following any changes to the computerised system.
Change Management	Change management is the process of controlling the life cycle of changes.
Commercial off-the-shelf (COTS) product	Software or hardware is a commercial off-the-shelf (COTS) product if provided by a vendor to the general public, if available in multiple and identical copies, and if implemented by the test facility management without or with some customization.
Computerised System	"A computerized system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel." *PIC/S PI 11-3 "Good Practices for Computerised Systems in Regulated GxP Environments*" 

Configuration	A configuration is an arrangement of functional units and pertains to the choice of hardware, software and documentation. It affects function and performance of the system.
Configuration Management	Configuration management comprises those activities necessary to be able to precisely define a computerised system at a certain time point.
Controlled function	Is a process or operation integrated with a computer system and performed by trained people.
Corrective and Preventive Actions	The concept of corrective and preventive actions focusses on the systematic investigation of the root causes of identified problems or risks in an attempt to prevent their recurrence or to prevent occurrence.
Customized computerised system	A computerised system individually designed to suit a specific business process.
Data (derived data)	Derived data depend on raw data and can be reconstructed from raw data (e.g., final concentrations as calculated by a spreadsheet relying on raw data, result tables as summarized by a LIMS, etc.).
Data (raw data)	Data (raw data) may be defined as measurable or descriptive attribute of a physical entity, process or event. The GLP Principles define raw data as all laboratory records and documentation, including data directly entered into a computer through an automatic instrument interface, which are the results of primary observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study.
Data approval	Data approval means locking data after collection, verification and e.g. transformation to make data suitable for use in records.
Data capture	Data capture are actions that typically take place to plan, collect, and verify data and associated metadata elements.
Data migration	Data migration is the activity of e.g. transporting electronic data from one computer system to another, transferring data between storage media or simply the transition of data from one state to another [e.g. conversion of data to a different format]. The term “data” refers to “raw data” as well as “metadata”.
Deviation (incident) management	Deviation (incident) management comprises those activities to identify, document, evaluate and when appropriate, investigate in order to determine the originating causes of deviation (incident) to prevent recurrence.
Electronic record	Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
Electronic Signature	An electronic measure that can be substituted for a handwritten signature or initials for the purpose of signifying approval, authorisation or verification of specific data entries.

Hybrid solution (system)	Co-existence of paper and electronic record and signature components. Examples include combinations of paper (or other non-electronic media) and electronic records, paper records and electronic signatures, or handwritten signatures linked to electronic records.
Life cycle	An approach to computerised system development that begins with identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends when use of the system is retired.
Life cycle model	A life cycle model describes the phases or activities of a project from conception until the product is retired. It specifies the relationships between project phases, including transition criteria, feedback mechanisms, milestones, baselines, reviews, and deliverables.
Metadata	Metadata is data about data. Metadata is any information used for the identification, description, and relationships of electronic records or their elements. Metadata gives data meaning, provides context, defines structure, and enables retrievability across systems, and usability, authenticity, and auditability across time.
Operating System	A programme or collection of programmes, routines and sub-routines that controls the operation of a computer. An operating system may provide services such as resource allocation, scheduling, input/output control, and data management.
Peripheral Components	Any interfaced instrumentation, or auxiliary or remote components such as printers, modems and terminals, etc.
Process	A process is a series of actions designed to produce a specified result. A process defines required activities and the responsibilities of the personnel assigned to do the work. Appropriate tools and equipment, procedures and methods define the tasks and relationships between the tasks.
Qualification	Action of proving that any equipment including software operates correctly and is fit for its purpose.
Recognised Technical Standards	Standards as promulgated by national or international standard setting bodies (ISO, IEEE, ANSI, etc.)
Regulated record	Is one required to be maintained or submitted by GLP regulations. A regulated record may be held in different formats, for example, electronic, paper, or both.
Risk	Combination of the probability of occurrence of harm and the severity of that harm.
Risk analysis	Estimation of the risk associated with the identified hazards. It is the qualitative or quantitative process of linking the likelihood of occurrence and severity of harms.
Risk assessment	Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards. Risk

	assessment is followed by risk control.
Risk control	Process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.
Risk identification	A systematic use of information to identify hazards referring to the risk question or problem description. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.
Risk management	The concept of quality risk management is described as “a systematic process” for the assessment, control, communication and review of risks to the quality.
Risk mitigation	Actions taken to lessen the probability of occurrence of harm and the severity of that harm.
Security	The protection of computer hardware and software from accidental or malicious access, use, modification, destruction or disclosure. Security also pertains to personnel, data, communications and the physical and logical protection of computer installations.
Software	A programme acquired for or developed, adapted or tailored to the test facility requirements for the purpose of controlling processes, data collection, data manipulation, data reporting and/or archiving.
Source Code	An original computer programme expressed in human-readable form (programming language) which must be translated into machine-readable form before it can be executed by the computer.
User requirement specifications	User requirement specifications define in writing what the user expects the computerised system to be able to do.
User review	Review of user access rights and privileges
Validation	Action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring and demonstrating the fitness for its purpose.
Validation strategy	The validation strategy defines in a document the process and all activities related to each stage of validation of computerised system.

Further definitions of terms can be found in the "*OECD Principles of Good Laboratory Practice.*"