OECD DRAFT ADVISORY DOCUMENT 16[1]

THE APPLICATION OF GLP PRINCIPLES TO COMPUTERISED SYSTEMS

FOREWARD

1. The following draft Advisory Document will replace the 1995 OECD GLP Consensus Document number 10 - *The Application of the Principles of GLP to Computerised Systems.* The original Document 10 was developed by the OECD Working Group on GLP, based on a document emanating from a 1992 workshop held in Switzerland. The current Draft Advisory Document, also developed by the Working Group, retains all of the key text from the original Consensus Document 10 where changes were unnecessary, but also includes new text to reflect the current state-of-the art in this field. This draft will be revised based on the input received during the public comment period.

PREAMBLE

2. This document introduces a life-cycle based validation approach, emphasizing risk assessment as the central element of a scalable, economic and effective validation approach. The intention is to give regulatory guidance in developing an adequate validation strategy for any type of computerised system in a GLP environment regardless of its complexity.

1. GENERAL

1.1. Scope and definition of terms

3. All computerised systems used for the generation, measurement or assessment of data intended for regulatory submission should be developed, validated, operated and maintained in ways which are compliant with the GLP Principles.

4. During the planning, conduct and reporting of studies there may be several computerised systems in use for a variety of purposes. Such purposes might include the direct or indirect capture of data from automated instruments, operation/control of automated equipment and the processing, reporting and storage of data. For these different activities, computerised systems can vary from a programmable analytical instrument, or a personal computer to a laboratory information management system (LIMS) with multiple functions. Whatever the scale of computer involvement, the GLP Principles should be applied.

5. This guidance applies to all types of computerised systems used in GLP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. Hardware is the physical components of the computerised system; it will include the computer unit itself and its peripheral components. Software is the programme or programmes that control the operation of the computerised system. All GLP Principles which apply to equipment therefore apply to both hardware and software.

[1] This document would replace OECD Consensus Document *No 10: The Application of the Principles of GLP to Computerised Systems* (1995)

6. Computerised systems should be of appropriate design, adequate capacity and suitable for their intended purposes. There should be appropriate procedures to control and maintain these systems, and the systems should be developed, validated and operated in a way which is in compliance with the GLP Principles.

7. The demonstration that a computerised system is suitable for its intended purpose is of fundamental importance and is referred to as computer validation.

8. The validation process provides 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.

9. This guidance regulates any computerised system, regardless of its complexity (it covers the range from simple devices like balances to complex systems like laboratory information management systems). Validation is required for the process or a sub-process performed by a computerised system. Validation should only be carried out on qualified IT infrastructure. The process should be reliable and able to perform according to the intended purpose based on qualified hardware and software.

10. The validation approach should be life cycle based giving the regulated user the freedom to choose any life cycle model. The regulated user's life cycle approach should entail defining and performing activities in a systematic way from conception, understanding the requirements, through development, release, operational use, to system retirement. Life cycle activities should be scaled based on justified risk assessment decisions. Minimal activities might 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.

11. Validation of newly established computerised systems should be done prospectively. Validation should include testing and change control within the production environment. Retrospective validation should be carried out for existing systems (legacy systems) that have become GLP relevant. Guidance for the validation of legacy systems is given by PIC/S PI 11-3 "Good Practices for Computerised Systems in Regulated GxP Environments" [effective 25.09.2007].

1.2. Risk Assessment

12. Risk assessment should be applied throughout the life cycle of a computerised system taking into account data integrity and the quality of the study results. Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment. It should interact with other relevant procedures (e.g. configuration and change management, data management).

13. Risk assessment may be part of a test facility's risk management system. It should be a key instrument to develop an adequate validation strategy and to scale the validation efforts. The validation effort should be driven by the intended GLP relevant use of the system and its risks to data quality and integrity. The outcome of the risk assessment processes should result in the assignment of appropriate validation activities to computerised systems or computerised system functionalities. This is of paramount importance for an effective validation approach and economic (scaled) validation decisions giving the regulated user an adequate instrument to validate simple laboratory systems as well as complex laboratory data management systems properly.

14. Dual use system (have both GLP and non-GLP uses and functions) would still require development, validation, operation, and retirement under GLP change control and security.

1.3. Personnel, roles and responsibilities

15. The GLP Principles require that a test facility has appropriately qualified and experienced personnel and that there are documented 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 provisions should also apply for all personnel involved with computerised systems.

16. Management of a test facility has the overall responsibility for compliance with the GLP Principles. This includes the responsibility to establish policies and procedures to ensure that computerised systems are validated in order to demonstrate that systems suit their intended purpose and are operated and maintained in accordance with the Principles of GLP. This responsibility includes the appointment and effective organisation of an adequate number of appropriately qualified and experienced staff, as well as the obligation to ensure that the facilities, equipment and data handling procedures are of an adequate standard. Management is responsible for ensuring that computerised systems are suitable for their intended purposes. Management should also ensure that policies and procedures relevant to achieve and maintain the validated status are understood and followed, and ensure that effective monitoring of compliance occurs. Management should also 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.

17. Involvement of study directors and quality assurance in any validation-relevant tasks is essential to achieve and maintain a system's validated status.

18. The Study Directors are responsible under the GLP Principles for the overall conduct and GLP compliance of their studies. The Study Directors should be fully aware of the involvement of any computerised system used in studies under their direction. Study Directors have the responsibility to ensure that computerised systems used in their studies are validated. The Study Director’s responsibility for data recorded electronically is the same as that for data recorded on paper.

19. Quality Assurance (QA) personnel should monitor the GLP compliance of computerised systems and verify for a specific study the valid use of computerised systems. QA responsibilities for computerised systems should be defined by management and described in written policies and procedures. The quality assurance program should include procedures and practices that will assure that established standards are met for all phases of the validation, operation and maintenance of computerised systems. Procedures and practices should cover the whole life-cycle of purchased as well as in-house developed systems. Quality Assurance personnel should be given training in any specialist techniques necessary. Quality assurance should audit validation and verify the valid use of a computerised system. They should be sufficiently familiar with such systems so as to permit relevant comment; in some cases the appointment of specialist auditors may be necessary. Quality Assurance personnel should have, for data review, direct read-only access to the data stored within a computerised system.

20. Study directors and quality assurance personnel should have sufficient training to understand their relevant procedures in validation, use and maintenance of computerized systems. Involvement of system owners, process owners and quality assurance in any validation-relevant tasks is essential to achieve and maintain a system's validated status (e.g. change and configuration management).

21. Personnel who develop, validate, operate, use and maintain computerised systems are responsible for performing their activities in accordance with the GLP Principles and recognized technical standards. The test facility should define roles and responsibilities for both validation activities and operation of the system. The definition of roles should be adequate and complete and it may be risk-based (even a simple system should be dealt with by adequately defined key personnel). To validate a system and operate a validated system there should be close cooperation between all relevant

personnel such as the Process Owner (e.g. Study Director, Head of Analytical Department, etc.), System Owner, Quality Assurance personnel and IT personnel. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. Personnel in any particular role should have suitable experience, system knowledge, and training. For example, a system owner or a validation director should understand the adequacy of the validation approach. The person's training and experience should correlate in a plausible way with the complexity of the validation project (minimal training for simple systems / processes; in depth training / experience for complex systems / processes).

22. The regulated user should pay close attention to interactions between the roles in validation as well as operation. For example, appropriate support should be given to the validation personnel by the system owner and process owners; the tasks of quality assurance in validation as well as in operation of the system should be laid down in SOPs.

23. In the operational phase of a specific study, roles and responsibilities should correlate with system access privileges, training and general GLP requirements. Training records and system access authorizations of users should be available to demonstrate sufficient knowledge to fulfill the role in a computerised system in a GLP compliant manner.

24. Potential incompatibilities of roles and responsibilities should be considered to avoid risks to data integrity (if the system owner and process owner are the same person, the control of the audit trail might be in the hands of a person using the system).

Roles and responsibilities are summarized in table 1.

1.4. Facilities

25. 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.

26. 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.

27. Adequate facilities should be provided for the secure retention of electronic storage media.

1.5. Supplier and Service Provider

28. When suppliers (e.g. third parties, vendors, internal IT departments, service providers including hosted service providers) are used to provide, install, configure, integrate, validate, maintain, modify or retain a computerised system or related service or for data processing, formal agreements must exist between the GLP facility and any third parties. These agreements should include clear statements of the responsibilities of the third party.

29. For vendor-supplied systems it is likely that much of the documentation created during the development is retained at the vendor’s site. In this case, evidence of formal assessment and/or vendor audits should be available at the test facility.

30. A written agreement should exist for any provided system. Depending on the system’s complexity and the involvement of the supplier in purchase, validation and operation of the system the agreement should be detailed appropriately.

31. The regulated user should define the interfaces between his quality assurance / risk management / validation system and the activities provided by a third party. Such interface should be applicable to the validation phase as well as operation of a system. For example, Installation Qualification and/or Operational Qualification of an HPLC system performed by the vendor should be evaluated by the facility's validation system.

32. Suppliers need not conform to GLP regulations, but must operate to a documented quality system verified as acceptable by the quality assurance unit of the regulated user. The test facility should have proper documentation or regulate by contract if documentation is kept at the vendor's site.

33. Hosted services (e.g. platform, software, archiving, backup or processes as a service) should be treated like any other third party service and require written agreements. It is the responsibility of the regulated user to evaluate the relevant service and to estimate risks to data integrity and data availability. The regulated user should be aware of potential risks resulting from the uncontrolled use of hosted services.

34. The regulated user may treat the GLP test facility's internal IT department as a third party service provider. A test facility may include the company IT department as a full part of its GLP Facility and reporting to the Test Facility Management, or as a contracted third party. The responsibilities should be defined in a written manner for any system which requires the activity of the internal IT-department.

35. The competence and reliability of a supplier or service provider should be evaluated. The need for an audit should be based on a documented risk assessment. The regulated user should be able to provide information about the quality systems of suppliers and developers where considered necessary.

36. Efforts in evaluating a service provider should be linked to the complexity and criticality of a system (e.g. a LIMS or any bespoke software provided from external sources might need greater attention). It is the regulated user's responsibility to justify the type of the audit of a service provider or the omission of an audit, based on a risk assessment. An audit that covers technical as well as compliance issues requires the involvement of competent validation personnel (e.g. system owner and/or validation director) and quality assurance.

1.6. Commercial off-the-shelf Products

37. Documentation supplied with commercial off-the-shelf (COTS) products should be reviewed by regulated users to check that user requirements are fulfilled.

38. The regulated user should be able to justify if a COTS product (e.g. spread-sheet applications, statistics package, data capturing package) is able to cover defined user requirements (e.g. by referencing in the user requirement specifications the technical capabilities of the COTS according to the user manual).

39. Spreadsheet templates for calculations using pre-defined formulas or self-written code should be regarded as an in-house developed application. As the qualification of the underlying COTS product has no relevance for the application, validation and documentation according chapter 2 and 3 is required.

40. Providers of computer operating systems or other COTS would not be subject to auditing, and their products would require qualification rather than validation.

1.7. Change and configuration management

41. Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

42. Change control and configuration management procedures should cover the validation phase, the operational phase and the phase in which the system is retired. If a computerised system is used for archiving, the system should be considered as operational as long as it holds GLP relevant data.

43. Change and configuration management should correlate with the software's category, system's complexity and its criticality to data integrity. Software categorization may carried out as recommended in chapter 15 of PIC/S PI 11-3 "Good Practices for Computerised Systems in Regulated GxP Environments" (effective 25.09.2007).

44. The circumstances of study specific data capturing, data calculation and data release should correlate with a particular system's configuration at any relevant point in time within a study. GLP key personnel (process owner and quality assurance) should be involved in any changes to GLP relevant systems.

45. Change and configuration management should be linked to risk assessment, testing, release and documentation procedures.

1.8. Documentation

46. All relevant phases of the life-cycle should be documented. Depending on the computerized system, this may include purchase, specification, design, development and validation, implementation, operation and retirement. There should be written management policies covering, *inter alia*, the acquisition, requirements, design, validation, testing, installation, operation, maintenance, staffing, control, auditing, monitoring and retirement of computerised systems.

47. Some OECD Member countries require that the source code for application software should be available at, or retrievable to, the test facility.

48. For each application there should be documentation fully describing:

a) The name of the application software or identification code and a detailed and clear description of the purpose of the application.
b) The hardware (with model numbers) on which the application software operates.
c) The operating system and other system software (e.g., tools) used in conjunction with the application.
d) The application programming language(s) and/or data base tools used.
e) The major functions performed by the application
f) An overview of the type and flow of data/data base design associated with the application.
g) File structures, error and alarm messages, and algorithms associated with the application.
h) The application software components with version numbers.
i) Configuration and communication links among application modules and to equipment and other systems.

49. Much of the documentation covering the use of computerised systems will be in the form of SOPs. These should cover, but not be limited to, the following:

a) Procedures for the operation of computerised systems (hardware/software), and the responsibilities of personnel involved.

b) Procedures for security measures used to detect and prevent unauthorised access and programme changes.
c) Procedures and authorisation for programme changes and the recording of changes.
d) Procedures and authorisation for changes to equipment (hardware/software) including testing before use if appropriate.
e) Procedures for the periodic testing for correct functioning of the complete system or its component parts and the recording of these tests.
f) Procedures covering both routine preventative maintenance and fault repair. These procedures should clearly detail the roles and responsibilities of personnel involved.
g) Procedures for software development and acceptance testing, and the recording of all acceptance testing.
h) Back-up procedures for all stored data and contingency plans in the event of a breakdown.
i) Procedures for the archiving and retrieval of all documents, software and computer data.
j) Procedures for the monitoring and auditing of computerised systems.

50. Documentation activities should be integrated in a quality management system and should cover all GLP relevant computerized systems. The depth of documentation may correlate with the complexity and the validation strategy of the computerized system. All relevant management policies, validation and operational procedures should be described in SOPs. Such SOPs may comprise but are not limited to: risk assessment; service management; validation planning; specification; verification (qualification testing); reporting and release; document management; traceability; incident, change and configuration management; periodic review, security management and record management.

51. Records should be generated to reconstruct proper validation and use of the computerized system. Such records may comprise but are not limited to: risk assessment; supplier assessment; service level agreements; requirement specifications; test records; release records; personnel and user training; incident, change and configuration records and records of use.

52. The complete documentation of validation and use of a specific 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. Inventory

53. An up-to-date listing of all GLP-relevant systems and their functionality (inventory) should be maintained. Study-relevant computerised systems should be traceable from the study plan or relevant method to the inventory.

54. The regulated user should have a comprehensive list of all GLP relevant systems indicating their validation status. The list should cover non-GLP-relevant systems as well to enable the evaluation of the regulated user's GLP criticality assessment.

2.2. Validation

55. Computerised systems should be designed to satisfy GLP Principles and introduced in a pre-planned manner. The validation, its documentation and reports should cover the relevant steps of the life-cycle. The relevant steps should be defined by the regulated user based on the complexity and intended use of a system. The regulated user should be able to justify standards, protocols, acceptance criteria, procedures and records based on risk assessment.

56. Retrospective evaluation: There will be systems where the need for compliance with GLP Principles was not foreseen or not specified. Where this occurs there should be documented justification for use of the systems; this should involve a retrospective evaluation to assess suitability. Retrospective evaluation begins by gathering all historical records related to the computerised system. These records are then reviewed and a written summary is produced. This retrospective evaluation summary should specify what validation evidence is available and what needs to be done in the future to ensure validation of the computerised system.

57. There should be evidence that the system was adequately tested for conformance with the acceptance criteria 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.

58. The regulated user should define the life cycle, the depth of a validation, the relevant phases, the corresponding deliverables and the acceptance criteria based on risk assessment. The validation effort may be scaled and adapted to the type of system. The scaling should be justified. The regulated user may rely on best practice guidance when scaling the validation effort. For example, the regulated user`s validation deliverables may be limited to user requirements specifications, a validation plan, a performance qualification and a validation report if it can be justified by risk assessment.

2.3. Change control during validation phase

59. Validation documentation should include change control records (if applicable) and reports of any GLP critical deviations observed during the validation process.

60. A change control and a deviation management system should be in place beginning with the validation phase. Validation documentation should include change control records and records about the management of deviations. If a **(**bespoke**)** system is developed by a vendor, it is the regulated user`s responsibility to ensure change control and deviation management in the development phase.

61. If such records are not considered relevant it should be justified by the regulated user based on a risk assessment (e.g. a simplified validation approach of a less complex [simple] system).

2.4. System description

62. 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.

63. An up-to-date system description should be maintained throughout the life cycle of the system. In the instance of simple systems with low complexity, user requirement specifications or another document may describe the system sufficiently.

2.5. User requirement specifications (URS)

64. URS should be generated for any computerised system. URS should describe the functions of a system and should be based on a documented risk assessment. URS should be traceable throughout the life-cycle.

65. URS are of paramount importance for all validation activities and should be generated for all GLP relevant computerised systems regardless of the system`s complexity (e.g. the regulated user`s perspective of a simple spread sheet used to calculate concentration data should be described by URS). URS 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 URS should be traceable to any further specification documents (e.g. functional specifications) and test documents throughout the whole life-cycle.

66. If a provided system (purchased or hosted by a third party) contains more functions than needed, those functions should be identified which are GLP relevant and need to be tested.

67. URS should also be available for retrospectively validated systems.

2.6. Quality Management System and Support Procedures

68. A computerised system should be developed, validated and operated in accordance with an appropriate quality management system. In order to ensure that a computerised system remains suitable for its intended purpose, support mechanisms should be in place to ensure the system is functioning and being used correctly. This may involve system management, training, maintenance, technical support, auditing and/or performance assessment.

69. Any computerised system regardless of its complexity and regardless of the validation approach should be validated within the scope of a quality management system. There should be adequate documentation that each system was developed in a controlled manner and preferably according to recognised quality and technical standards (e.g. ISO/9001). Both the development of a computerised system as well as the validation project should be integrated in quality management systems. If a system is developed by a vendor, it is the responsibility of the regulated user to evaluate the vendor`s systems development quality management system. The regulated user should rely on a risk assessment when defining the evaluation strategy.

2.7. Bespoke Systems

70. There should be a process in place for the validation of bespoke or customized computerised systems that ensure the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

71. This requirement applies to systems which are developed for a specific application of a particular customer (e.g. GLP study specific data capturing systems, spread sheet templates with formulas or macros, queries, statistical applications or data evaluation systems, etc.). Such applications may also be configured or coded specifically for one or more GLP studies. As no experience can be drawn from the market acceptance, bespoke systems bear the highest intrinsic risk.

72. If such a system is provided by a supplier, the interface between supplier and regulated user, and the quality system of the supplier, are of paramount importance.

73. The validation effort of the regulated user should consider all quality relevant activities of the supplier even at the supplier's business location. Outsourced activities or in-house supplier activities should be part of the applications life-cycle.

74. If a hosted application is a coded or configured application, the rules apply analogously.

75. Source code of bespoke systems should be retrievable by the regulated user to provide the monitoring authority access to the software code.

2.8. Testing

76. Evidence of appropriate test methods and test scenarios should be demonstrated. In particular, system (process) parameter limits, data limits and error handling should be considered.

77. Qualification testing [e.g. DQ (Design Qualification); IQ (Installation Qualification); OQ (Operational Qualification); and PQ (Performance Qualification)] should be carried out to ensure that a system meets its requirements. Such testing should check those areas where GLP data integrity is at risk. All systems, including purchased systems (e.g. an HPLC system), need to be tested and evaluated by the regulated user. It is the regulated user's responsibility to decide on the depth and breadth of the testing efforts. Decisions of the regulated user on testing should be guided by a risk assessment. Supplier testing may assist the regulated user in their validation efforts. It is the regulated user’s responsibility to understand the need for testing and to ensure the completeness of the tests and test documentation. Testing should be based upon proper testing procedures, clearly defined roles and responsibilities as well as documentation standards.

78. The regulated user should consider a method specific PQ to demonstrate the GLP study specific fitness of a system (e.g. prove the suitability of a system to determine a particular analyte concentration range with defined specificity, accuracy and precision).

79. In case testing leads to changes of the system, an interface to change control procedures should exist. It is the regulated user's responsibility to have evidence of proper testing regardless of whether the testing is done by the regulated user or by a supplier. Evidence could be provided by maintaining records of internal testing results, or records of vendor auditing.

2.9. Data Migration

80. Where system obsolescence forces a need to transfer electronic raw data from one system to another, then the process must be well documented and its integrity verified. If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. Conversion of data to a different format should be considered as data migration (e.g. from a proprietary raw data format to PDF).

81. Where such migration is not practicable then the raw data must be transferred to another medium and this verified as an exact copy prior to any destruction of the original electronic records.

82. Data migration is the activity of transporting electronic data from one system to another, or simply the transition of data from one state to another (e.g. conversion of raw data to a different format). Data migration may occur in the course of a GLP study or after a study project has been finished. Data migration should be part of the regulated user's validation scope if GLP relevant data are affected regardless of the status of any GLP study project. If study records are archived in an electronic system, data migration may become relevant.

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

a) In-place version upgrades.
b) Data conversions (from one supplier database to another).
c) Same system migration (transporting application; data from one server to another).
d) Migration from a source to a target system.

84. Migrated data should remain usable and should retain its content and meaning. A risk assessment should be a key instrument in data migration. The regulated user should ensure the meaningfulness of a system audit trail and electronic signatures after migration. It is the regulated user's responsibility to maintain the link between the readable audit trail or electronic signatures and the audited data.

3. OPERATIONAL PHASE

85. All computerised systems should be installed and maintained in a manner which ensures the continuity of accurate performance.

3.1. Exchange of Data

86. Communications related to computerised systems broadly fall into two categories: between computers or between computers and peripheral components. All communication links are potential sources of error and may result in the loss or corruption of data. Appropriate controls for security and system integrity must be adequately addressed during the development, validation, operation and maintenance of any computerised system.

87. Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. GLP-relevant data may be transported automatically, uni-directional or bi-directional, from one system to another system (e.g. from a remote data capturing system into a central data base, from spread sheets into a LIMS, from a chromatography data management system into a LIMS, or from a spread sheet into a statistics software application). The regulated user should consider any automatic data flow and any data processing during automatic data transport. To minimize any risks to data quality the regulated user should establish such interfaces as part of the validation effort and based on a risk assessment.

88. Note: This requirement is not meant to require validation of standard transfer infrastructure and its procedures (e.g. TCP/IP).

3.2. Accuracy checks

89. For any critical data which is manually entered into a system, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

90. The regulated user should identify all GLP relevant data entered manually into electronic systems. All potential risks to data if entered erroneously should be identified and risk mitigation strategies should be described.

91. If manual control procedures are applied, the efficacy and the ability to reconstruct such controls should be ensured. The adequate documentation of manual control activities is required.

92. If automatic control procedures are applied, any relevant control software should be validated (e.g. automatically applied validation scripts during data entry). The depth of validation efforts for control software should be scaled based on risk assessment.

93. Manual and automatic control procedures may be applied in combination. Documentation of manual control activities and validation of the automatic control should be considered proportionally.

94. It is the regulated user`s responsibility to adequately control any electronic data entry systems regardless of its complexity, and to consider the impact of such systems on data quality and data integrity. The use of unvalidated data entry systems should be excluded (e.g. uncontrolled copies of spreadsheets or unauthorised reuse of validated spreadsheets).

3.3 Data and storage of data

95. When raw data are stored electronically it is necessary to establish long term retention requirements for the type of data and the expected life of computerised systems. Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. Hardware and software system changes must provide for continued access to, and retention of, the raw data without integrity risks. Supporting information such as maintenance logs and calibration records that are necessary to verify the validity of raw data or to permit reconstruction of a process or a study should be retained in the archives.

96. Regular back-ups of all relevant data and software should be carried out to allow recovery of the system following any failure which compromises the integrity of the system. A back-up copy may become raw data and must be treated as such. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.

97. The regulated user should have:

a) identified all GLP-relevant electronic records (raw data, derived data and any other study relevant electronic data);
b) assessed the impact of the records on the quality of study results;
c) assessed potential risks to the records;
d) established risk-based risk mitigation procedures, and
e) controlled the effectiveness of risk mitigation.

98. For any GLP-relevant computerised system the regulated user should identify all electronic records consisting of raw data and derived data

99. Raw data. The GLP Principles define raw data as being all original laboratory records and documentation, including data directly entered into a computer through an instrument interface, which are the results of original observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study.

100. Computerised systems operating in compliance with the GLP Principles may be associated with raw data in a variety of forms, for example electronic storage media, computer or instrument printouts and microfilm/fiche copies. It is necessary that raw data are defined for each computerised system.

101. Primary observations entered into a computerised system manually or captured automatically by a computerised system may include weight data as recorded by balances, areas under the curve as captured by a chromatography data management system, configuration data of an analytical instrument to prove the circumstances under which analytical raw data were captured, etc.

102. Derived data depend on raw data (e.g., final concentrations as calculated by a spreadsheet, result tables as summarized by a LIMS, written observations and conclusions as written by a pathologist, etc.).

103. Risk based procedures 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. barriers controlling and monitoring access of personnel to server rooms etc.);
b) protection of storage media against loss or destruction (e.g. fire, humidity, destructive electricity, theft, etc.);
c) logical 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);
d) protection of stored 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);
e) ensuring accessibility and readability of data by providing an adequate physical environment as well as software environment.

104. These aspects of data storage should be considered within each computerised system for specific impact on the GLP study specifically during the study phase and in the archiving period. It is not necessary to have an evaluation included in the study documentation. However, the test facility should have a documented overview of how data are stored, how these requirements are fulfilled and which studies are affected. If the test facility hands over the electronic study data to a sponsor, the responsibility for the electronic study data migrates to the sponsor.

3.4. Printouts

105. It should be possible to print all electronic records (including raw data and derived data) as well as metadata (all electronic information required to interpret raw data and derived data). This includes all information about changes done to records, if such changes are relevant for the correct content and meaning.

106. If entered data are modified post-entry, and if the modification could have an impact on the results, the system should automatically mark such data appropriately and the mark should be dis-

played on the screen and in printed copies. The original data should be stored together with the modified data; for example, any calculated chromatogram modified for the purpose of recalculation should be marked irrevocably.

3.5. Audit trails

107. Audit trails need to be available and convertible to a human readable form and regularly reviewed.

108. The regulated user should identify GLP relevant electronic records based on a risk assessment. The regulated user should audit such electronic data to record all user activities resulting in changes and deletions. Each change must not obscure the original entry. It should be possible to reconstruct all data before a change / deletion based on the time stamp of the change / deletion, the name of the person executing the change / deletion and the rationale for the change / deletion.

109. If audit policies for the application system are provided by the supplier, these should be enabled and set up properly to reflect the roles and responsibilities of GLP study personnel. Modifications to the audit trail settings should be restricted to authorised personnel by proper system authorisation and change control concepts. Process owners (e.g. GLP study directors, heads of analytical departments) or users (e.g. any GLP study personnel [analysts]) should not be authorised to change audit trail settings.

110. A system should be in place that ensures the periodic review of the audit trail system and the recorded information. For example, the regulated user should periodically review the completeness and current suitability of the audit trail system as well as the user behavior based on the recorded information. GLP quality assurance personnel should be involved in the review process.

111. The existence of an audit trail of changes and deletions may be obvious by annotation or formatting when viewing data, or may exist as a record of changes independent of the view to the data.

3.6. Change and Configuration Management

112. Change control is the formal approval and documentation of any change to the computerised system during the operational life of the system. Change control is needed when a change may affect the computerised system's validation status. Change control procedures must be effective once the computerised system is operational. Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure. The regulated user should understand that configuration management is closely related and interwoven with change control in order to demonstrate a system composition at any time of the life cycle.

113. Where maintenance activities have necessitated changes to hardware and/or software it may be necessary to validate the system again.

114. The regulated user should have appropriate procedures for change control and configuration management during the operational phase. Procedures should describe the method of evaluation to determine the extent of retesting necessary to maintain the validated state of the system. Clearly defined roles and responsibilities as well as risk assessment procedures should be in place. 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.

115. Any modification or repair to a computerised system, for whatever reason (e.g. for maintenance purposes; in response to incidents; for facility/study specific purposes) should be traceable to

appropriate change and configuration control records. After any modification or repair, the valid status of the system should be verified and documented.

116. Modifications implemented by routine automation (e.g., virus protection or operating system patches) should be within the system description and need not be part of change management.

117. Sufficient records are required to demonstrate the adequate use of any computerised system during operation or within a GLP study (e.g. the compliance of an analytical instrument's configuration with the method validation requirements) – regardless of its complexity.

118. Any GLP study result should be traceable to the relevant and valid system configuration to allow the verification of settings as provided by the study plan or the relevant (analytical) method.

119. Any exclusion from a change management system should be justified within the system risk assessment.

3.7. Periodic evaluation

120. Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GLP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

121. The frequency and depth of the periodic evaluation procedures should be determined based on a risk assessment considering complexity and GLP criticality. The suitability of the evaluation activities should be ensured by involving key players (e.g. GLP quality assurance, system owner, process owner, validation and IT personnel). The need for an interface between the periodic evaluation activities and an incident reporting system may be considered depending on a risk assessment.

122. Performance assessment is the formal review of a system at periodic intervals to ensure that it continues to meet stated performance criteria, e.g., reliability, responsiveness, capacity.

123. The test results and assessment of periodic evaluations should be documented.

3.8. Physical, logical security and data integrity

124. Documented security procedures should be in place for the protection of hardware, software and data from corruption or unauthorised modification, or loss. Physical and/or logical controls should be in place to restrict access or changes to a computerised system as well as to the data held within the system to authorised persons. Suitable physical and logical methods of preventing unauthorised entry 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 computer equipment and data storage areas. Creation, change, and cancellation of access authorisations should be recorded.

125. For equipment not held within specific ’computer rooms’ (e.g., personal computers and terminals), standard test facility access controls are necessary as a minimum. However, where such equipment is located remotely (e.g., portable components and modem links), additional measures need to be taken.

126. It is essential to ensure that only approved versions of software are in use. Logical security may include the need to enter a unique user identity with an associated password. Any introduction of data or software from external sources should be controlled. These controls may be provided by the

computer operating system software, by specific security routines, routines embedded into the applications or combinations of the above. Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

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

128. Since maintaining data integrity is a primary objective of the GLP Principles, it is important that everyone associated with a computerised system is aware of the necessity for the above security considerations. 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.

129. Considering complexity and criticality of a system, as well as the requirements of the organisation in which the system is operated, appropriate physical and/or logical controls should be implemented. If necessary, the regulated user should establish physical controls like access controls to interfaces, computers or server rooms.

130. Appropriate and well maintained authorization concepts should specify logical access rights to domains, computers, applications and data. User privileges should be defined for operating systems as well as applications, and should be adapted as required by the organization of the facility in combination with the requirements of a particular GLP study. Roles and responsibilities of personnel granting user privileges should be defined.

131. User privileges should be defined specifically for GLP studies if necessary. Incompatibilities of GLP study activities and user privileges should be considered (e. g. the laboratory role 'analyst' might not be compatible with the role 'administrator' in a chromatography data management system).

132. 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. Procedures about changes of entered electronic data and authorisation of data changes not already monitored by automated audit trail should be defined.

133. Roles and user privileges in computerised systems should reflect the organizational requirements of GLP studies.

134. The regulated user is responsible for appropriate training of users. Training activities should be documented.

3.9. Incident Management

135. During the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken. All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions. Incident review should be part of a periodic evaluation.

136. The regulated user should define the term “incident” and should be able to categorise the GLP criticality of “incidents” for all computerised systems based on a risk assessment. Depending on the criticality appropriate root cause analysis, corrective / preventative actions should be taken. GLP

quality assurance, system owner and if appropriate, the study director and the sponsor, should be involved. It should be possible to trace all incidents reported for a computerised system to the affected GLP studies. The documentation of a GLP study should contain enough information to trace all relevant incidents with a computerised system to the incident management system. Incident records should be maintained with the system documentation, and archived at retirement of the system. Depending on the criticality of an incident, copies of all incident relevant records should be archived with the documentation of the affected studies.

137. The regulated user should consider incident management as element of change management, configuration management and the periodic review program.

3.10. Electronic signature

138. Electronic records may be signed electronically. Electronic signatures are expected to:

a) have the same legal consequences as a hand-written signatures within the boundaries of the test facility,
b) be permanently linked to their respective record(s), and
c) include the time and date that they were applied.

139. The regulated user should have a policy about the approval of records and should have identified those records which require a signature by the applicable regulations.

140. The regulated user has the discretion to decide when to use an electronic signature.

141. If electronic records are signed electronically, procedures should be in place to identify the relevant electronic records and the personnel authorized to sign electronically. The authorized personnel should be clearly identifiable and bound by name to the internal electronic signature policy. Facility management, study director and quality assurance should ensure the establishment of an adequate electronic signature system and ensure its adequate maintenance and use. It might be necessary to adapt signature privileges to study specific requirements.

142. An adequately established and closely monitored authorisation concept for the relevant computerised systems should be a prerequisite of any electronic signature system.

143. The regulated user should ensure that the handwritten signature is equivalent to the electronic signature and its authenticity is indisputable. 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. Records which are associated with the electronic signature should be clearly identified. For example, the electronic signature of a chromatogram covers all other electronic records which impact the chromatogram such as method setting, system configuration etc.; changes to such records influence the meaning of the signature in the chromatogram). A risk based control system should ensure the timeliness of the linkage between the electronically signed record and the supporting records.

144. Any change to an electronically signed record or to the applied signature (including the linkage to the signed record) should be detectable. Such signatures should not be accepted.

145. 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 (and supporting records, if applicable) within the archiving period should be possible and subjected to periodic evaluation.

146. The regulated user may apply a paper based procedure to sign records that are maintained electronically. Such hybrid solution should be described clearly to identify all records which are represented by the signed paper record. An appropriate system for version control should ensure the timeliness of the linkage between the signed paper record and the electronic records. The use of modified or out-of-date records should be excluded. A risk assessment considering the impact of the records should be applied when designing the control process. If a complete set of electronic records and its printed analogue are maintained in parallel, the regulated user should specify the regulated record type in order to apply appropriate control procedures.

3.11. Data approval and data release

147. When a computerised system is used for the recording and approval of GLP relevant data, the system should allow only authorised personnel to release data and it should clearly identify and record the person releasing the data.

148. Electronic release of data should be performed using an electronic signature.

149. The electronic data approval / release process should be documented in detail. The relevant computerised systems as well as the roles and responsibilities of involved personnel should be identified and traceable to study specific requirements. The linkage between an affected GLP study and the applied electronic data approval / release procedure should be part of the GLP study documentation.

3.12. Archiving

150. The GLP Principles for archiving data must be applied consistently to all data types. It is therefore important that electronic data are stored with the same levels of access control, indexing and expedient retrieval as other types of data.

151. GLP study data may be archived electronically. The data should be accessible and readable, and its integrity maintained, during the archiving period. Where electronic data from more than one study are stored on a single storage medium (e.g., disk or tape), a detailed index will be required.
If relevant changes are to be made to the archiving system (e.g. computer equipment or programs), the continuing ability to retrieve the data should be ensured and tested.

152. It may be necessary to provide facilities with specific environmental controls appropriate to ensure the integrity of the stored electronic data. If this necessitates additional archive facilities then management should ensure that the personnel responsible for managing the archives are identified and that access is limited to authorised personnel. It will also be necessary to implement procedures to ensure that the long-term integrity of data stored electronically is not compromised. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring that continued readability of the data should be established. This may, for example, include producing hard copy printouts or transferring the data to another system.

153. No electronically stored data should be destroyed without management authorisation and relevant documentation. Other data held in support of computerised systems, such as source code and development, validation, operation, maintenance and monitoring records, should be held for at least as long as study records associated with these systems.

154. Electronic archiving should be regarded as a separate process which has to be appropriately validated (a read only electronic storage system is not considered as an archive). A risk assessment should be applied when designing the archiving procedure. The archivist, who holds sole responsibility, may delegate tasks during the management of electronic records to competent personnel or automated processes (e.g., access control). For roles and responsibilities in the archiving process refer to

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

155. The regulated user should identify all relevant electronic records of a GLP study which are subject to electronic archiving.

156. If a hybrid solution is chosen (i.e. paper records and electronic records in parallel) the regulated user should specify the regulated version of a record for relevance in archiving.

157. As content and meaning of an electronic record should be preserved during the archiving period, the complete information package should be identified and archived (e.g. electronic signatures, audit trails, any other meta-data necessary to understand the meaning of a record correctly or to reconstruct its source).

158. If migration of data including conversion to a different data format is relevant, the requirements of this guidance on data migration should be met. This includes processes intended to copy data to a different data media.

159. Relevant data formats and hosting systems should be evaluated regarding accessibility, readability and influences on data integrity during the archiving period.

160. If data media, data formats, hardware or software of archival systems (not the data-collection systems) change during the archiving period, the regulated user should ensure that there is no influence on the accessibility, readability and integrity of the records during the archiving period. A risk assessment, change control, configuration management and test management should be considered as relevant standard procedures when changes in the archiving system are required.

3.13 Business continuity and disaster recovery

161. Provisions should be made to ensure the continuity of support for computerised systems which support critical processes in the event of a system breakdown (e.g. a manual or alternative computerised system).

162. The time required to bring the alternative arrangements into use should be based on risk and should be appropriate for a particular system and the business process it supports.

163. These arrangements should be adequately documented and tested.

164. In case an alternative data capture procedure is applied, the circumstances of any manually recorded raw data subsequently entered into the computer should be clearly identified as such, and should be retained as the original record. Manual back-up procedures should serve to minimise the risk of any data loss and ensure that these alternative records are retained.

165. 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 a paper-based 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. Personnel involved in the conduct of studies according to the GLP Principles should be aware of such contingency plans.

166. Procedures for the recovery of a computerised system will depend on the criticality of the system, but it is essential that back-up copies of all software are maintained. If recovery procedures entail changes to hardware or software, the validation requirements of this guidance apply.

167. An alternative computerised system should meet the validation requirements of this guidance. The change should have no negative impact on data quality.

Table 1: Roles and Responsibilities

It is the responsibility of the regulated user to avoid conflicts between roles.

Role	Responsibility
Test facility management	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.3.)
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.)
Quality Assurance	(*See* ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.8.)
User	The personnel operating the computerised system.
Regulated user	The regulated entity, that is responsible for the GLP compliant operation of a computerised system and the applications, files and data held thereon. The regulated entity is the test facility, represented by the test facility management.
Personnel	Any person involved in validation, operation or support of a computerised system.
Process Owner	The individual who is ultimately responsible for ensuring that the computerised system and its operation is in compliance with GLP and fit for intended use in accordance with applicable SOPs. (GAMP 5). In a GLP test facility this is the test facility management.
System 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 SOPs. The system owner also may be the process owner. 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. (GAMP 5)
Validation Director	A delegated person responsible for a validation project.
IT Personnel	Personnel involved in the purchase, installation and operation of a computerised system. Responsibility includes, for example, operating and maintaining the hardware and software, conducting backups, resolving problems, etc.
System Engineer	IT personnel responsible for technical aspects (e.g., change control) of a specific computerised system.
System Archivist	Delegated personnel technically responsible for the archiving of data from a specific computerised system working on behalf of the GLP archivist.
Supplier	Third parties, vendors, internal IT departments, service providers including hosted service providers, etc.
Third Party	Parties not directly managed by the test facility management.

Table 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.
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.
Bespoke / Customized computerised system	A computerised system individually designed to suit a specific business process.
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.
Computer System:	Computer hardware components assembled to perform in conjunction with a set of software programs (applications), which are collectively designed to perform a specific (controlled) function or group of (controlled) functions. (See also Figure 1, page 8, of PIC/S Good Practices for Computerised Systems in Regulated GxP Environments [effective 25.09.2007]).
Computerised System	A computer system plus the controlled function that it operates.
Controlled function:	Is a process or operation integrated with a computer system and performed by trained people.
Electronic Signature:	The entry in the form of magnetic impulses or computer data compilation of any symbol or series of symbols, executed, adapted or authorised by a person to be equivalent to the person's handwritten signature.
GAMP5:	Good Automated Manufacturing Practice (GAMP 5 - A risk based approach to compliant computerized systems) © ISPE 2007
Hardware:	The physical components of a computerised system, including the computer unit itself and its peripheral components.
Life cycle concept:	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 discontinued.
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.
Legacy System:	These are regarded as systems that have been established and in use for many years. For a variety of reasons, they may be generally characterised by a lack of adequate GLP compliance related documentation and records pertaining to the development and commissioning stage of the system. Additionally, because of their age, no records may exist which describe a formal approach to validation of the system.
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.
Sub process	A part of the process which contributes to the result of the whole (e.g. a data capturing interface which transports data from a chromatography data management system to a laboratory data management system).
Qualification:	Action of proving that any equipment including software operates correctly and is fit for its purpose.
Design Qualification	Documented verification that the proposed design is suitable for the intended purpose. (GAMP5)
Installation Qualification	Documented verification that a system is installed according to written and pre-approved specifications. (GAMP5)
Operational Qualification	Documented verification that a system is operated according to written and pre-approved specifications throughout specified operation ranges. (GAMP5)
Performance Qualification	Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written pre-approved specifications, within the scope of the business process and operating environment. (GAMP5)
Recognised Technical Standards:	Standards as promulgated by national or international standard setting bodies (ISO, IEEE, ANSI, etc.)
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.
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 (Application):	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.
Software (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.
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.
Validation of a Computerised System:	The demonstration that a computerised system is suitable for its intended purpose.
Validation:	Action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring the fitness for its purpose.

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