Working document QAS/16.667
May 2016
Draft document for comment

World Health Organization

GUIDELINES ON VALIDATION – APPENDIX 5
VALIDATION OF COMPUTERIZED SYSTEMS
(May 2016)

DRAFT FOR COMMENTS

Should you have any comments on the attached text, please send these to Dr S. Kopp, Group Lead, Medicines Quality Assurance, Technologies, Standards and Norms (kopps@who.int) with a copy to Ms Marie Gaspard (gaspardm@who.int) by **12 July 2016**.

Medicines Quality Assurance working documents will be sent out electronically only and will also be placed on the Medicines website for comment under "Current projects". If you do not already receive our draft working documents please let us have your email address (to bonnyw@who.int) and we will add it to our electronic mailing list.

© World Health Organization 2016

All rights reserved.

This draft is intended for a restricted audience only, i.e. the individuals and organizations having received this draft. The draft may not be reviewed, abstracted, quoted, reproduced, transmitted, distributed, translated or adapted, in part or in whole, in any form or by any means outside these individuals and organizations (including the organizations' concerned staff and member organizations) without the permission of the World Health Organization. The draft should not be displayed on any website.

Please send any request for permission to:

Dr Sabine Kopp, Group Lead, Medicines Quality Assurance, Technologies, Standards and Norms, Regulation of Medicines and other Health Technologies, Department of Essential Medicines and Health Products, World Health Organization, CH-1211 Geneva 27, Switzerland. Fax: (41-22) 791 4730; email: kopps@who.int.

The designations employed and the presentation of the material in this draft do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the World Health Organization in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by the World Health Organization to verify the information contained in this draft. However, the printed material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the World Health Organization be liable for damages arising from its use.

This draft does not necessarily represent the decisions or the stated policy of the World Health Organization.

Draft for comment

SCHEDULE FOR THE PROPOSED ADOPTION PROCESS OF DOCUMENT QAS/16.667:

GUIDELINES ON VALIDATION – APPENDIX 5
VALIDATION OF COMPUTERIZED SYSTEMS

Discussion of proposed need for revision in view of the current trends in validation during informal consultation on data management, bioequivalence, GMP and medicines' inspection	29 June–1 July 2015
Preparation of draft proposal for revision of the main text and several appendices by specialists in collaboration with the Medicines Quality Assurance Group and Prequalification Team (PQT)-Inspections, based on the feedback received during the meeting and from PQT-Inspections, draft proposals developed on the various topics by specialists, as identified in the individual working documents.	July 2015–April 2016
Presentation of the progress made to the fiftieth meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations	12–16 October 2015
Discussion at the informal consultation on good practices for health products manufacture and inspection, Geneva	4–6 April 2016
Preparation of revised text by Mrs M. Cahilly and Dr A.J. van Zyl, participants at the above-mentioned consultation, based on Mrs Cahilly's initial proposal and the feedback received during and after the informal consultation by the meeting participants and members of PQT-Inspections	May 2016
Circulation of revised working document for public consultation	May 2016
Consolidation of comments received and review of feedback	August–September 2016
Presentation to the fifty-first meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations	17–21 October 2016
Any other follow-up action as required	…

Draft for comment

Background information

The need for revision of the published *Supplementary guidelines on good manufacturing practices: validation* (World Health Organization (WHO) Technical Report Series, No. 937, 2006, Annex 4) *(1)* was identified by the Prequalification of Medicines Programme and a draft document was circulated for comment in early 2013. The focus of the revision was the Appendix on non-sterile process validation (Appendix 7), which had been revised and was adopted by the Committee at its forty-ninth meeting in October 2014 *(2)*.

The main text was sent out for consultation as *Working document QAS/15.639* entitled *"Guidelines on Validation*" which constitute the general principles of the new guidance on validation.

The draft on the specific topics, the appendices to this main text, will follow. One of them, i.e. the ***Validation of computerized systems,*** *constitutes this working document.*

The following is an overview on the appendices that are intended to complement the general text on validation:

Appendix 1
Validation of heating, ventilation and air-conditioning systems
→ will be replaced by cross-reference to WHO Guidelines on GMP for HVAC systems for considerations in qualification of HVAC systems
(update - working document QAS/15.639/Rev.1) (2)

Appendix 2
Validation of water systems for pharmaceutical use
→ will be replaced by cross-reference to *WHO Guidelines on water for pharmaceutical use for consideration in qualification of water purification systems (3)*

Appendix 3
Cleaning validation – consensus to retain

Appendix 4
Analytical method validation – update in process

Appendix 5
Validation of computerized systems – updated text proposed in this working document

Appendix 6
Qualification of systems and equipment – update in process

Appendix 7
Non-sterile process validation – update already published as Annex 3, WHO Technical Report Series, No. 992, 2015

Draft for comment

VALIDATION OF COMPUTERIZED SYSTEMS

Contents

Draft for comment

1. INTRODUCTION AND SCOPE

1.1 Computerized systems should be validated at the level appropriate for their intended use and in accordance with quality risk management principles. This applies to systems used in all good (anything) practices (GXP) activities (e.g. good clinical practice (GCP), good laboratory practice (GLP) and good manufacturing practices (GMP)) *(3)*.

1.2 The purpose of validation of a computerized system is to ensure an acceptable degree of documented evidence that establishes confidence in the accuracy, reliability and consistency in performance of the system in accordance with predetermined specifications. The validation data should meet the principles of being attributable, legible, contemporaneous, original and accurate (ALCOA) throughout the data life cycle.

1.3 Computerized system validation should ensure that all necessary technical and procedural controls are implemented ensuring compliance with good documentation practices for electronic data generated by the system (WHO guidance on good data and record management practices, WHO Technical Report Series, No. 996, Annex 5, 2016) *(4)*.

1.4 System elements that need to be considered in computerized system validation include computer hardware and software, related equipment and network components and operating system environment, procedures and systems documentation including user manuals and people (such as, but not limited to, users, data reviewers, system application administrators, network engineers, database administrators and people involved in archiving). Computerized system validation activities should address both system configuration as well as any custom-developed elements.

1.5 Computerized systems should be maintained in the validated state with risk-based controls appropriate to the different stages of the system life cycle. These stages include system planning, specification, programming and configuration, system testing, preparation and verification of standard operating procedures (SOPs) and training programmes, system operation and maintenance including handling of software and hardware updates, monitoring and review, followed by system retirement.

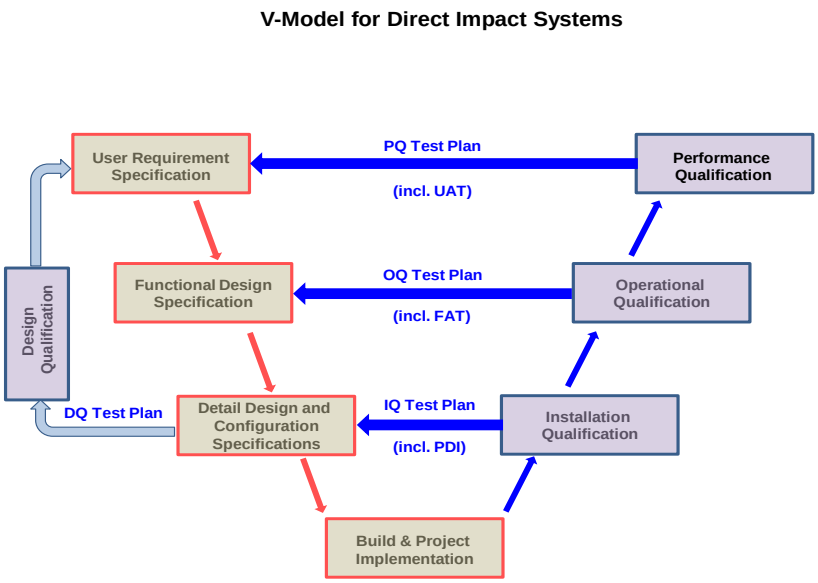
1.6 Depending on the types of systems or typical applications such as process control systems (distributed control system (DCS), programmable logic controller (PLC), supervisory control and data acquisition (SCADA)), laboratory information management systems (LIMS), laboratory instrument control systems and business systems (enterprise resource planning (ERP), manufacturing resource planning (MRP II)) used by the manufacturer, a document covering (but not limited to) the following information should be available on-site:

Draft for comment

- purpose and scope;
- roles and responsibilities;
- validation approach;
- risk management principles;
- system acceptance criteria;
- vendor selection and assessment;
- computerized system validation steps;
- configuration management and change control procedures;
- back-up and recovery;
- error handling and corrective action;
- contingency planning and disaster recovery;
- maintenance and support;
- system requirement;
- validation deliverables and documentation;
- template, formats, annex; examples.

1.7 A typical model for computerized systems validation is the V-model. The lifecycle development model (or V-model for short), is a framework or structure for undertaking the design, execution and commissioning of a design project (see also International Society for Pharmaceutical Engineering (ISPE) Baseline: a risk based approach to compliant GXP computerized systems GAMP). The left-hand edge of the V is where the project is defined and specified in greater detail. The bottom point of the V is the execution step of the project. The right-hand edge of the V is where the commissioning and qualification testing of the installed system is performed. The V-model provides a logical sequence that helps to organize the complex activities of defining a project scope, executing it and qualifying it.

Draft for comment



2. GLOSSARY

archival. Archiving is the process of protecting records from the possibility of being further altered or deleted, and storing these records under the control of independent data management personnel throughout the required retention period. Archived records should include, for example, associated metadata and electronic signatures.

audit trail. The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the "who, what, when and why" of the action.

For example, in a paper record, an audit trail of a change would be documented via a single-line cross-out that allows the original entry to remain legible and documents the initials of the person making the change, the date of the change and the reason for the change, as required to substantiate and justify the change. In electronic records, secure, computer-generated, time-stamped audit trails should allow for reconstruction of the course of events relating to the creation, modification and deletion of electronic data. Computer-generated audit trails should

Draft for C

retain the original entry and document the user identification, the time/date stamp of the action, as well as the reason for the change, as required to substantiate and justify the action. Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system, specific electronic records or specific data contained within the record.

backup. A backup means a copy of one or more electronic files created as an alternative in case the original data or system are lost or become unusable (for example, in the event of a system crash or corruption of a disk). It is important to note that backup differs from archival in that back-up copies of electronic records are typically only temporarily stored for the purposes of disaster recovery and may be periodically overwritten. Such temporary back-up copies should not be relied upon as an archival mechanism.

business continuity plan. A written plan that is documented and maintained that defines the ongoing process supported by management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure the continuity of services through personnel training, plan testing and maintenance.

change control. The process of assuring that a computerized system remains validated following a change. It includes assessing the impact of the change to determine when and if repetition of a validation or verification process or specific portion of it is necessary and performing appropriate activities to ensure the system remains in a validated state.

cloud based. Comments invited.

computerized system. A computerized system collectively controls the performance of one or more automated processes and/or functions. It includes computer hardware, software, peripheral devices, networks and documentation, e.g. manuals and standard operating procedures, as well as the personnel interfacing with the hardware and software, e.g. users and information technology
support personnel.

computerized systems validation. Means confirmation by examination and provision of objective evidence that computer system specifications conform to user needs and intended uses and that all requirements can be consistently fulfilled.

configuration management. A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a

Draft for comment

configuration item, control changes to those characteristics, record and report change processing and implementation status and verifying compliance with specified requirements.

COTS. Commercial off-the-shelf software; a vendor-supplied software component of a computerized system for which the user cannot claim complete software life-cycle control.

data. Data means all original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, which are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GXP activities is recorded.

data governance. The totality of arrangements to ensure that data, irrespective of the format in which they are generated, are recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data life cycle.

data integrity. Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, such that they are attributable, legible, contemporaneously recorded, original or a true copy and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.

data life cycle. All phases of the process by which data are created, recorded, processed, reviewed, analysed and reported, transferred, stored and retrieved and monitored until retirement and disposal. There should be a planned approach to assessing, monitoring and managing the data and the risks to those data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle.

disaster recovery. Process for planning or engaging appropriate resources to restore the normal business function in the event of a disaster.

dynamic record format. Records in dynamic format, such as electronic records, that allow for an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user (with proper access permissions) to reprocess the data and expand the baseline to view the integration more clearly.

Draft for comment

functional specifications. The functional specifications document, if created, defines functions and technological solutions that are specified for the computerized system based upon technical requirements needed to satisfy user requirements (e.g. specified bandwidth required to meet the user requirement for anticipated system usage).

good documentation practices. In the context of these guidelines, good documentation practices are those measures that collectively and individually ensure documentation, whether paper or electronic, is secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.

GXP. Acronym for the group of good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biologicals and medical devices, such as good laboratory practices, good clinical practices, good manufacturing practices, good pharmacovigilance practices and good distribution practices.

installation qualification or installation verification testing. Documented verification that a system is installed according to written specifications for design and configuration.

master data. Comments invited.

metadata. Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. Metadata necessary to evaluate the meaning of data should be securely linked to the data and subject to adequate review. For example, in weighing, the number 8 is meaningless without metadata, i.e. the unit, mg. Other examples of metadata include the time/date stamp of an activity, the operator identification (ID) of the person who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.

operational qualification or operational/functional verification testing. Documented verification that a system operates according to written operational specifications throughout specified operating ranges.

performance qualification or performance/requirements verification testing. Documented verification that a system is capable of performing or controlling the activities of the processes it is required to perform, according to written user requirements and specifications, in its intended business and computing environment.

Draft for comment

production environment. The business and computing operating environment in which a computerized system is used by end-users. For regulated computerized systems, the production environment is the business and computing operating environment in which the computerized system is being used for good laboratory practice-regulated purposes.

regression analysis and testing. A software verification and validation task to determine the extent of verification and validation analysis and testing that must be repeated when changes are made to any previously examined software component or system.

static record format. A static record format, such as a paper or PDF record, is one that is "fixed" and allows no or very limited interaction between the user and the record content. For example, once printed or converted to static PDFs, chromatography records lose the capability of being reprocessed or enabling more detailed viewing of baselines or any hidden fields.

system life cycle. The period of time that starts when a computerized system is conceived and ends when the product is no longer available for use by end-users. The system life cycle typically includes a requirements and planning phase; a development phase that includes: a design phase and a programming and testing phase; and a system qualification and release phase that includes: system integration and testing phase; system validation phase; system release phase; and a system operation and maintenance phase; and a system retirement phase.

user acceptance testing. Verification of the fully-configured computerized system installed in the production environment (or in a validation environment equivalent to the production environment) to perform as intended in the automated business process when operated by end-users trained in end-user standard operating procedures (SOPs) that define system use and control. User-acceptance testing may be a component of the performance qualification (PQ) or a validation step separate from the PQ.

user requirements specification. The user requirements specification (URS), if prepared as a separate document, is a formal document that defines the requirements for use of the software system in its intended production environment.

verification. The act of reviewing, inspecting, testing, checking, auditing or otherwise establishing and documenting whether or not items, processes, services or documents conform to specified requirements.

Draft for comment

3. COMPUTERIZED SYSTEM VALIDATION MASTER PLAN, PROTOCOLS AND REPORTS

3.1 There should be a computerized system validation master plan that describes the policy, approach, organization and planning, resources, execution and management of computerized system validation for all of the GXP systems in use on-site.

3.2 The computerized system validation master plan (CSVMP) should contain, for example, the scope, risk management approach and a complete inventory list of all GXP systems. The CSVMP should also outline the controls including but not limited to backup and recovery of data, contingency planning, disaster recovery, change control management, configuration management, error handling, maintenance and support, corrective measures and system access control policies, that will be in place to maintain the validated state of the systems.

3.3 The CSVMP should refer to protocols and reports as appropriate, for the conduct of validation.

3.4 Where appropriate, computerized systems should be classified based on risk assessment relating to their GXP impact.

Validation protocol

3.5 Validation should be executed in accordance with the validation protocol and applicable SOPs.

3.6 A validation protocol should define the validation strategy, including roles and responsibilities and documentation and activities to be performed. The protocol should cover the specification, development, testing, review and release of the computerized system for GXP use.

3.7 The validation protocol should be tailored to the system type, impact, risks and requirements applicable to the system in which it will be used.

Validation report

3.8 A validation summary report should be prepared, summarizing system validation activities.

3.9 It should outline the validation process and activities and describe and justify any deviations from the process and activities specified in the protocol.

Draft for comment

3.10 The report should include all critical and major test discrepancies that occurred during the verification/validation testing and describe how these were resolved.

3.11 The report should be approved after the resolution of any issue identified during validation and the system should then be released and ready for GXP use.

4. VENDOR MANAGEMENT

4.1 For vendor-supplied and/or vendor-managed computerized systems or system components, including cloud-based systems, an evaluation of the vendor-supplied system and the vendor's quality systems should be conducted and recorded. The scope and depth of this evaluation should be based upon risk management principles.

4.2 Vendor evaluation activities may include: completion of an audit checklist by the vendor; gathering of vendor documentation related to system development, testing and maintenance including vendor procedures, specifications, system architecture diagrams, test evidence, release notes and other relevant vendor documentation; and/or on-site audit of the vendor facilities to evaluate and continuously monitor as necessary the vendor's system life-cycle control procedures, practices and documentation.

4.3 Appropriate quality agreements should be in place with the vendor defining the roles and responsibilities and quality procedures throughout the system life cycle.

5. REQUIREMENTS SPECFICATIONS

5.1 Requirements specifications should be written to document the minimum user requirements and functional or operational requirements and performance requirements. Requirements may be documented in separate URS and functional requirements specifications (FRS) documents or in a combined document.

User requirements specifications

5.2 The authorized URS document, or equivalent, should state the intended uses of the proposed computerized system and should define critical data and data life-cycle controls that will assure consistent and reliable data throughout the processes by which data is created, processed, transmitted, reviewed, reported, retained and retrieved and eventually disposed.

5.3 The URS should include requirements to ensure that the data will meet regulatory requirements such as ALCOA principles and WHO guidelines on good documentation practices.

Draft for comment

5.4 Other aspects that should be specified include, but are not limited to, those related to:

- the data to be entered, processed, reported, stored and retrieved by the system, including any master data and other data considered to be the most critical to system control and data output;
- the flow of data including that of the business process(es) in which the system will be used as well as the physical transfer of the data from the system to other systems or network components. Documentation of data flows and data process maps are recommended to facilitate the assessment and mitigation and control of data integrity risks across the actual, intended data process(es);
- networks and operating system environments that support the data flows;
- how the system interfaces with other systems and procedures;
- the limits of any variable and the operating programme and test programme.
- synchronization and security control of time/date stamps;
- technical and procedural controls of both the application software as well as operating systems to assure system access only to authorized persons;
- technical and procedural controls to ensure that data will be attributable to unique individuals (for example, to prohibit use of shared or generic login credentials);
- technical and procedural controls to ensure that data is legibly and contemporaneously recorded to durable ("permanent") media at the time of each step and event and controls that enforce the sequencing of each step and event (for example, controls that prevent alteration of data in temporary memory in a manner that would not be documented);
- technical and procedural controls that assure that all steps that create, modify or delete electronic data will be recorded in independent, computer-generated audit trails or other metadata or alternate documents that record the "what" (e.g. original entry), "who" (e.g. user identification), "when" (e.g. time/date stamp) and "why" (e.g. reason) of the action;
- backups and the ability to restore the system and data from backups;
- the ability to archive and retrieve the electronic data in a manner that assures that the archive copy preserves the full content of the original electronic data set, including all metadata needed to fully reconstruct the GXP activity. The archive copy should also preserve the meaning of the original electronic data set, including its dynamic format that would allow the data to be reprocessed, queried and/or tracked and trended electronically as needed;
- input/output checks, including implementation of procedures for the review of original electronic data and metadata, such as audit trails;
- technical and procedural controls for electronic signatures;
- alarms and flags that indicate alarm conditions and invalid and altered data in order to facilitate detection and review of these events;

Draft for comment

- system documentation, including system specifications documents, user manuals and procedures for system use, data review and system administration;
- system capacity and volume requirements based upon the predicted system usage and performance requirements;
- performance monitoring of the system;
- controls for orderly system shutdown and recovery;
- business continuity.

Note: For specific applications, in addition to general requirements, the URS should have specific requirements.

5.5 User requirements should be related to the tests carried out in the qualification phase (typically either the operation qualification (OQ) or the PQ)

5.6 In the case of, e.g. a chromatography data system (CDS), it is further important to define the requirements for the basic functions of taking into account following details:

- requirements for hardware, workstations and operating systems;
- system requirements such as number of users, locations;
- compliance requirements, i.e. open or closed system, security and access configuration, data integrity, time and date stamp, electronic signature and data migration;
- workflow of CDS;
- information technology (IT) support requirements;
- interface requirements.

Functional specifications

5.7 The functional specifications should define specific functions of the computerized system based upon technical requirements needed to satisfy user requirements.

5.8 The functional specifications provide a basis for the system design and configuration specifications. Functional specifications should consider requirements for operation of the computerized system in the intended computing environment, such as network infrastructure requirements, as well as functions provided by vendor-supplied software as well as functions required for user business processes that are not met by out-of-the-box software functionality and default configurations and that will require custom code development.

5.9 With regard to the proper functioning of computer software, the following general aspects should be kept in mind when specifying installation and user/functional requirements:

Draft for comment

- language, name, function (purpose of the programme);
- inputs;
- outputs, including electronic data and metadata that constitute the "original records";
- fixed set point (process variable that cannot be changed by the operator);
- variable set point (entered by the operator);
- edits (reject input/output that does not conform to limits and minimize errors);
- input processing parameters (and equations);
- programme overrides (e.g. to stop a mixer before time).

5.10 The personnel access roles who have the ability and/or are authorized to write, alter or have access to programmes should be identified. There should be appropriate segregation of roles between personnel responsible for the business process and personnel in system administration and maintenance roles who will have the ability to alter critical master data, critical set points, and system policies and configuration settings.

5.11 With regard to the proper functioning of computer hardware and to prevent damage, the following general aspects should be kept in mind when specifying installation and functional requirements:

- location;
- power supply;
- environmental conditions;
- magnetic disturbances;
- mechanical disturbances;
- physical security.

6. SYSTEM DESIGN AND CONFIGURATION SPECIFICATIONS

6.1 System design and configuration specifications should be developed based on user and functional requirements. Specification of design parameters and configuration settings (separate or combined) should ensure data integrity and compliance with "good documentation practices for electronic data".

6.2 System design and configuration specifications should provide a high-level system description as well as an overview of the system physical and logical architecture and should map out the automated system business process and relevant work flows and data flows if these have not already been documented in other requirements specifications documents.

6.3 The system design and configuration specifications may include, as applicable,

Draft for comment

specifications to define design of software code, for software code that is developed in-house, if any, and configuration specifications of configurable elements of the software application, such as security profiles, audit trail configuration, data libraries and other configurable elements.

6.4 In addition, the system design and configuration specifications may also include, based upon risk, the hardware design and configuration specifications as well as that of any supporting network infrastructure.

6.5 Example configuration settings and design controls for good documentation practices that should be enabled and managed across the computing environment (for both the software application, including off-the-shelf software, and operating systems environments) include, but are not limited to:

- restricting security configuration settings for system administrators to independent persons, where technically feasible;
- disabling configuration settings that allow overwriting and reprocessing of data without traceability;
- disabling use of "hidden fields" and the ability to delete data and the ability to obscure data with data annotation tools;
- restricting access to time/date stamps;
- for systems to be used in clinical trials, configuration and design controls should be implemented to protect the blinding of the trial, for example, by restricting access to who can view randomization data that may be stored electronically.

6.6 System design and configuration specifications should include secure, protected, independent computer-generated audit trails to track changes to these settings in the system.

7. DESIGN QUALIFICATION

7.1 A design review should be conducted to verify that the proposed design and configuration of the system is suitable for its intended purpose and will meet all applicable user and functional requirements specifications.

7.2 This process that may be referred to as design qualification, may include a review of vendor documentation, if applicable, and verification that requirements specifications are traceable to proposed design and configuration specifications.

8. BUILD AND PROJECT IMPLEMENTATION

8.1 Once the system requirements and the system design and configuration are specified and

Draft for comment

verified, system development or "build and test" activities may begin. The development activities may occur as a dedicated phase following completion of specification of system requirements and design and configuration (such as when adhering to a sequential or "waterfall" development model). Alternatively, development activities may occur iteratively as requirements are specified and verified (such as when prototyping or rapid-development methodologies are employed).

Vendor-supplied systems

8.2 For vendor-supplied systems, development controls for the vendor-supplied portion of the computerized system should be assessed during the vendor evaluation or supplier qualification. For custom-built systems and configurable systems, as well as for vendor-supplied systems that include custom components (such as custom-coded interfaces or custom report tools) and/or require configuration (such as configuration of security profiles in the software or configuration of the hardware within the network infrastructure), the system should be developed under an appropriate documented quality management system.

Custom-developed systems

8.3 For custom-developed systems or modules, the quality management system controls should include development of code in accordance with documented programming standards, review of code for adherence to programming standards and design specifications, and development testing that may include unit testing and module/integration testing.

8.4 System prototyping and rapid, agile development methodologies may be employed during the system build and development testing phase. There should be an adequate level of documentation of these activities.

Preparation for the system qualification phases

8.5 The system development and build phase should be followed by the system qualification phase. This typically consists of installation, operational and performance testing, but actual qualification required may vary depending on the scope of the validation project as defined in the validation plan and based upon a documented and justified risk assessment.

8.6 Prior to the initiation of the system qualification phase, the software program and requirements and specifications documents should be finalized and subsequently managed under formal change control.

8.7 Persons who will be conducting the system qualification should be trained to adhere to

Draft for comment

the following requirements for system qualification:

- test documentation should be generated to provide evidence of testing;
- test documentation should comply with good documentation practices;
- any discrepancies between actual test results and expected results should be documented and adequately resolved based upon risk prior to proceeding to subsequent test phases.

9. INSTALLATION QUALIFICATION

9.1 The first phase of system testing is installation qualification (IQ), also referred to as installation verification testing. IQ should provide documented evidence that the computerized system, including software and associated hardware, is installed and configured in the intended system testing and production environments according to written specifications.

9.2 The IQ will verify, for example, that the computer hardware on which the software application is installed has the proper firmware and operating system; that all components are present and in the proper condition; and that each component is installed per the manufacturer or developer instructions.

9.3 IQ should include verification that configurable elements of the system are configured as specified. Where appropriate, this could also be done during OQ.

10. OPERATIONAL QUALIFICATION

10.1 The OQ, or operational/functional verification resting, should provide documented evidence that the software and hardware function as intended throughout anticipated operating ranges.

10.2 Functional testing should include, based upon risk:

- an appropriate degree of challenge testing (such as boundary, range, limit, nonsense entry testing) to verify the system appropriately handles erroneous entries or erroneous use;
- verification that alarms are raised based upon alarm conditions;
- flags are raised to signal invalid or altered data.

Draft for comment

Considerations for functional testing of hardware and software

Note: the section below provides for examples, and is not an exhaustive list. Static, dust, power-feed voltage fluctuations and electromagnetic interference could influence the system.

Hardware

10.3 The extent of validation should depend on the complexity of the system. Appropriate tests and challenges to the hardware should be performed as part of validation.

10.4 Hardware is considered to be equipment and the focus should be on location, maintenance and calibration of hardware, as well as on qualification.

10.5 The qualification of the hardware should prove:

- that the capacity of the hardware matches its assigned function (e.g. foreign language);
- that it operates within the operational limits (e.g. memory, connector ports, input ports);
- that the hardware configuration settings are appropriate and meet user and functional requirements;
- that it performs acceptably under challenging conditions (e.g. long hours, temperature extremes);
- reproducibility/consistency.

10.6 Some of the hardware qualification may be performed by the computer vendor. However, the ultimate responsibility for the suitability of equipment used remains with the company.

10.7 Qualification protocols, reports (including data) should be kept by the company for the hardware in its configured state. When qualification information is produced by an outside firm, e.g. computer vendor, the records should be sufficiently complete (including general results and protocols) to allow the company to assess the adequacy of the qualification and verification activities. A mere certification of suitability from the vendor, for example, will be inadequate.

Software

10.8 Functional testing of software should provide assurance that computer programs (especially those that control critical activities in manufacturing and processing) will function consistently within pre-established limits for both normal conditions as well as under worst-case

Draft for comment

conditions (e.g. out-of-limit, out-of-range, alarm conditions).

10.9 Functional testing, also known as “black box” testing, involves inputting normal and abnormal test cases; then, evaluating outputs against those expected. It can apply to computer software or to a total system (reference: CEFIC GMP).

11. STANDARD OPERATING PROCEDURES AND TRAINING

11.1 Prior to the conduct of the PQ and user acceptance testing (UAT), and prior to the release of the computerized system for GXP use, there should be adequate written procedures and documents and training programmes created defining system use and control. These may include vendor-supplied user manuals as well as SOPs and training programmes developed in-house.

11.2 Example procedures and training programmes that should be developed include, but are not necessarily limited to:

- system use procedures that address:
  - routine operation and use of the system in the intended business process(es),
  - review of the electronic data and associated metadata (such as audit trails) and how the source electronic records will be reconciled with printouts, if any,
  - mechanisms for signing electronic data,
  - system training requirements prior to being granted system access;
- system administration procedures that address:
  - granting and disabling user access and maintaining security controls,
  - backup/restore,
  - archival/retrieval,
  - disaster recovery and business continuity,
  - change management,
  - incident and problem management,
  - system maintenance.

12. PERFORMANCE QUALIFICATION AND USER ACCEPTANCE TESTING

Note: The user requirements specifications should provide a basis for UAT that will be conducted by the system users during the PQ of the system.

12.1 PQ, that includes UAT, should be conducted to verify the intended system use and administration outlined in the URS, or equivalent document.

Draft for comment

12.2 The PQ should be conducted in the production environment or in a validation environment that is equivalent to the production environment in terms of overall software and hardware configuration.

12.3 PQ testing should also include, as applicable, an appropriate degree of stress/load/volume testing based upon the anticipated system use and performance requirements in the production environment.

12.4 In addition, an appropriate degree of end-to-end or regression testing of the system should be conducted to verify the system performs reliably when system components are integrated in the fully-configured system deployed in the production environment.

12.5 UAT should be conducted by system users to verify the adequacy of system use SOPs and data review SOP(s) and training programmes. The UAT should include verification of the ability to readily discern invalid and altered data, including the ability to efficiently review electronic data and metadata, such as audit trails.

12.6 IT system administrators should verify the adequacy of system administration SOP(s) and controls that will be routinely executed during normal operational use and administration of the system, including backup/restore and archival/retrieval processes.

Legacy systems

12.7 Comments invited.

13. SYSTEM OPERATION AND MAINTENANCE

Security and access control

13.1 Manufacturers should have systems and procedures in place to ensure security of data and control access to computerized systems.

13.2 Suitable security systems should be in place to prevent unauthorized entry or manipulation or deletion of data through both the application software as well as in operating system environments in which data may be stored or transmitted. Data should be entered or amended only by persons authorized to do so.

13.3 The activity of entering data, changing or amending incorrect entries and creating backups should be done in accordance with SOPs.

Draft for comment

13.4 Security should extend to devices used to store programs, such as tapes, disks and magnetic strip cards or other means. Access to these devices should be controlled.

13.5 Procedures for review of metadata, such as audit trails, should define the frequency, roles and responsibilities, and nature of these reviews.

13.6 Details on user profiles, access rights to systems, networks, servers, computer systems and software should be documented and an up-to-date list on the individual user rights for the software, individual computer systems and networks should be maintained and subjected to change control. The level of detail should be sufficient to enable computer system validation personnel, IT personnel/any external auditor/inspector to ascertain that security features of the system and of software used to obtain and process critical data cannot be circumvented.

13.7 All GXP computerized systems in a company, either stand-alone or in a network, should be monitored using an audit trail for the system that is configured to capture events that are relevant. These events should include all elements that need to be monitored to ensure that the integrity of the data could not have been compromised, such as but not limited to, changes in data, deletion of data, dates, times, backups, archives, changes in user access rights, addition/deletion of users and logins. The configuration and archival of these audit trails should be documented and also be subjected to change control. These audit trails should be validated to show that these cannot be modified in their archived form.

13.8 Actions, performance of the system and acquisition of data should be traceable and identify the persons who made entries and or changes, approved decisions or performed other critical steps in system use or control.

13.9 The entry of master data into a computerized system should be verified by an independent authorized person and locked before release for routine use.

13.10 Validated computerized systems should be maintained in the validated state once released to the GXP production environment.

13.11 There should be written procedures governing system operation and maintenance, including for example:

- performance monitoring;
- change management and configuration management;
- problem management;
- programme and data security;
- programme and data backup/restore and archival/retrieval;

Draft for comment

- system administration and maintenance;
- data flow and data life cycle;
- system use and review of electronic data and metadata (such as audit trails);
- personnel training;
- disaster recovery and business continuity;
- availability of spare parts and technical support;
- periodic re-evaluation.

13.12 Computerized systems should be periodically reviewed to determine whether the system remains in a validated state or whether there is a need for revalidation. The scope and extent of the revalidation should be determined using a risk-based approach. The review should at least cover:

- review of changes;
- review of deviations;
- review of incidents;
- systems documentation;
- procedures;
- training;
- effectiveness of corrective and preventive action (CAPA).

13.13 CAPA should be taken where indicated as a result of the periodic review.

13.14 Automatic updates should be subject to review prior to becoming effective.

14. SYSTEM RETIREMENT

14.1 Once the computerized system or components are no longer needed, the system or components should be retired in accordance with a change control procedure and formal plan for retirement.

14.2 Retirement of the system should include decommissioning of the software and hardware, retirement of applicable procedures as necessary. Measures should be in place to ensure the electronic records are maintained and readily retrievable throughout the required records retention period.

14.3 Records should be in a readable form and in a manner that preserves the content and meaning of the source electronic records. For example, if critical quality and/or compliance data need to be reprocessed after retirement of the system, the business owner may arrange for

Draft for comment

931 migration of the critical records to a new system and for verification of correct reprocessing of
932 the data on the new system.
933
934 14.4 The outcome of the retirement activities, including traceability of the data and
935 computerized systems, should be presented in a report.
936
937 **REFERENCES**
938
939 1. Supplementary guidelines on good manufacturing practice: validation. In: WHO Expert
940 Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva:
941 World Health Organization; 2006: Annex 4 (WHO Technical Report Series, No. 937).

942 2. Supplementary guidelines on good manufacturing practice: validation. Qualification of
943 systems and equipment. In: WHO Expert Committee on Specifications for Pharmaceutical
944 Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4,
945 Appendix 6 (WHO Technical Report Series, No. 937).

946 3. WHO good manufacturing practices for pharmaceutical products: main principles. In:
947 WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-eighth
948 report. Geneva: World Health Organization; 2014: Annex 2 (WHO Technical Report
949 Series, No. 986), also available on CD-ROM and online.

950 4. WHO guidance on good data and record management practices; 2016: Annex 5 (WHO
951 Technical Report Series, No. 996).

952 **Further reading**
953
954 Computerised systems. In: The rules governing medicinal products in the European Union.
955 Volume 4: Good manufacturing practice (GMP) guidelines: Annex 11. Brussels: European
956 Commission (http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-4/pdfs-
957 en/anx11en.pdf).
958
959 Drug Information Association. Computerized Systems Used in Nonclinical Safety Assessment;
960 Current Concepts in Validation and Compliance. Horsham, PA: Drug Information Association
961 (DIA), 2008.
962
963 GAMP® 5 – A Risk-Based Approach to Compliant GxP Computerized Systems. Tampa, FL:
964 GAMP Forum, International Society for Pharmaceutical Engineering (ISPE); 2008.
965
966 GAMP® good practice guide: A risk-based approach to GxP compliant laboratory computerized
967 systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE);
968 2012.

Draft for comment

GAMP® Good Practice Guide: A Risk-Based Approach to GxP Process Control Systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2011.

GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems – A Companion Volume to GAMP®5. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2010.

GAMP® Good Practice Guide: A Risk-Based Approach to Regulated Mobile Applications. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2014.

GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2012.

GAMP® Good Practice Guide: Global Information Systems Control and Compliance. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2005.

GAMP® Good Practice Guide: IT Infrastructure Control and Compliance. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2005.

GAMP® Good Practice Guide: Manufacturing Execution Systems – A Strategic and Program Management Approach. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2010.

MHRA GMP data integrity definitions and guidance for industry. London: Medicines and Healthcare Products Regulatory Agency; March 2015 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf).

National Institute of Standards and Technology, U.S. Department of Commerce, (NIST) Cloud Computing References: http://www.nist.gov/itl/cloud/index.cfm.

Official Medicines Control Laboratories Network of the Council of Europe: Quality assurance documents: PA/PH/OMCL (08) 69 3R – Validation of computerised systems – core document (https://www.edqm.eu/sites/default/files/medias/fichiers/Validation_of_Computerised_Systems_Core_Document.pdf) and its annexes:

- PA/PH/OMCL (08) 87 2R – Annex 1: Validation of computerised calculation systems: example of validation of in-house software
- (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_1_Validation

Draft for comment

_of_computerised_calculation.pdf).

- PA/PH/OMCL (08) 88 R – Annex 2: Validation of databases (DB), laboratory information management systems (LIMS) and electronic laboratory notebooks (ELN)
- (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_2_Validation_of_Databases_DB_Laboratory_.pdf).

- PA/PH/OMCL (08) 89 R – Annex 3: Validation of computers as part of test equipment (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_3_Validation_of_computers_as_part_of_tes.pdf)

Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic records; electronic signatures. US Food and Drug Administration. The current status of 21 CFR Part 11 Guidance is located under Regulations and Guidance at: http://www.fda.gov/cder/gmp/index.htm — see background: http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf.

PIC/S guide to good manufacturing practice for medicinal products annexes: Annex 11 – Computerised systems. Geneva: Pharmaceutical Inspection Co-operation Scheme.

PIC/S PI 011-3 Good practices for computerised systems in regulated GxP environments. Geneva: Pharmaceutical Inspection Co-operation Scheme

***

Draft for comment