Available online on 15 Sept, 2020 at https://ijdra.com/index.php/journal

International Journal of Drug Regulatory Affairs

Published by Diva Enterprises Pvt. Ltd., New Delhi
Associated with Delhi Pharmaceutical Sciences & Research University

Review Article

Importance of Qualification, Computer System Validation and its Regulatory Compliance in Pharmaceutical Industry

Neelu Jain, Sanjay Katre *, Anjaneyulu Vinukonda

Department of Science, Shri Satya Sai University of Technology and Medical Sciences, Sehore- (MP) - 466001

Abstract

In the pharmaceutical sector computer systems are integrated into the regular operations. The process or operation being controlled or monitored by the computer system, the procedural controls, and process related documentation, and the people. Computer systems performing regulated operations may control the quality of a product during its development, testing, manufacturing, and handling processes; manage information business operations; manage data used to prove the safety; efficacy and quality of the product and formulation. Systematic qualification and computer system validation helps to prevent software problems from production environment. A problem in a Pharmaceutical software application which affects the production environment can result in serious adverse consequence and also affect the product quality and business firm like lawsuits, financial penalties which ultimately results the company suffering from economic instabilities, staff downsizing and possibly eventual bankruptcy. The purpose of this industrial based research paper is to present and describe the steps as well as process involve in qualification and computer system validation of instrument/equipment used in pharmaceutical industry with current regulatory guidance.

Keywords: Computerised System Validation, Qualification, Regulatory Compliance, Risk Assessment, Good automated manufacturing practice (GAMP).

Article Info: Received 01 Sept. 2020; Review Completed 15 Sept. 2020; Accepted 15 Sept. 2020

Cite this article as:

Jain N, Katre S, Vinukonda A. Importance of Qualification, Computer System Validation and its Regulatory Compliance in Pharmaceutical Industry. International Journal of Drug Regulatory Affairs [Internet]. 15 Sept 2020 [cited 15 Sept 2020]; 8(3):70-77. Available from: http://ijdra.com/index.php/journal/article/view/411

DOI: 10.22270/ijdra.v8i3.411

*Corresponding author Tel.: +91-9949730770;
E-mail address: sckatre@gmail.com (Sanjay Katre).

1. Introduction

In 2002, the FDA adopted a risk based approach to regulatory compliance in pharmaceutical manufacturing when they started a review of their overall approach under the GMPs for the 21st Century programme. (1) As part of this programme, 21 CFR Part 11 was reassessed, the scope narrowed and industry was encouraged to adopt a risk based approach to interpretation of the regulation and validation of systems. Under this approach, risk assessment and risk management are key, but emerging, components of computerised system validation using the approach outlined in ISO 14971. (2, 3) GAMP and Computer system validation is define as below:

GAMP: Good automated manufacturing practice (GAMP) is both a technical subcommittee of the International Society for Pharmaceutical Engineering (ISPE) and a set of guidelines for manufacturers and users of automated systems in the pharmaceutical industry.

Computer system validation: It is process of 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. (4)

FDA General Principles of Software Validation

This Guidance for Industry, published by the FDA in 2002, is, in the opinion of the author, currently the best document on software validation written by the Agency. The essentials of risk management are contained in two main sections:

Section 4.8: Validation coverage should be based on the software's complexity and safety risk – not on firm size or resource constraints. The selection of validation activities, tasks, and work items should be commensurate with the complexity of the software design and the risk associated with the use of the software for the specified intended use. For lower risk devices, only baseline validation activities may be conducted. As the risk increases additional validation activities should be added to cover the additional risk.

Section 6.1: How Much Validation Is Needed?

The extent of validation evidence needed for such software depends on the device manufacturer's documented intended use of that software. For example, a device manufacturer who chooses not to use all the vendor-supplied capabilities of the software only needs to validate those functions that will be used and for which the device manufacturer is dependent upon the software results as part of production or the quality system. However, high-risk applications should not be running in the same operating environment with non-validated software functions, even if those software functions are not used.

Risk mitigation techniques such as memory partitioning or other approaches to resource protection may need to be considered when high-risk applications and lower risk applications are to be used in the same operating environment. When software is upgraded or any changes are made to the software, the device manufacturer should consider how those changes may impact the "used portions" of the software and must reconfirm the validation of those portions of the software that are used (see 21 CFR §820.70 (i)).

PIC/S Guidance for Computerised Systems

The Pharmaceutical Inspection Cooperation Scheme (PIC/S) has published guidance on 'Good Practices for Computerised Systems in GXP Environments' that provides good advice for risk management.

Section 4.3: For GXP regulated applications it is essential for the regulated user to define a requirement specification prior to selection and to carry out a properly documented supplier assessment and risk analysis for the various system options.

Section 23.7: GXP critical computerised systems are those that can affect product quality and patient safety, either directly (e.g. control systems) or the integrity of product related information (e.g. data/information systems relating to coding, randomisation, distribution, product recalls, clinical measures, patient records, donation sources, laboratory data, etc.). This is not intended as an exhaustive list. (5-8)

2. Importance of validation and qualification

Validation is a systematic approach where it is confirmed that any process in a pharmaceutical facility will operate within the specified parameters whenever required. This is achieved by collecting and analyzing data. Validation is done to assure that the processes will produce consistent and repeatable results within the predetermined specifications. Validation is needed as it verifies whether the quality standards and compliance are being met by the product in real time, which is really important in every pharmaceutical facility. Further, it also establishes that the facility is meeting current good manufacturing practice (cGMP) guidelines that are set for the industry by concerned regulatory bodies. Validation can be considered as a documented evidence of the process meeting the predetermined specifications.

Before you conduct validation, you must complete the process of qualification. It is a systematic process that starts by the project phases of the installations, equipment and utilities. Analytical Instrumentation Qualification, also known as AIQ, is the documented process where a complex and sophisticated measurement device is demonstrated to be accurate, precise and selective enough for the intended analytical measurement. This is carried out to determine the sustainability and qualification of any instrument for the intended purpose. Qualification is not limited to a validation process, but it is a part of it. It can be further divided into installation qualification (IQ), operation qualification (OQ) or performance qualification (PQ). Based on the operation and function of equipment, system or utility, you must make installation qualification and operation necessary. They should be monitored and calibrated periodically and they must be submitted to preventive maintenance.

No pharmaceutical plant is complete without an IT system, which is responsible for controlling, supporting and documenting various processes. It is extremely important to validate the computer and IT systems as it makes sure that all the concerned IT applications are fulfilling their intended purposes. Validation helps in controlling different phases of development, design, testing and routine of the software that is being used by the IT system during its life cycle. As long as the computer system is running accurately, you can be assured that all the information and reports that they store remain safe. You must implement stringent quality requirements in GMP-regulated industries to control the procedures throughout the Software Development Life Cycle (SDLC). Focus the validation efforts on crucial aspects such as risk analysis and in-depth validation approach. Make sure that you apply the documentation to the computerized system as it manages crucial data that has an impact on the quality of the products. The components of computer system validation include all the activities that are involved in applying the appropriate controls throughout the SDLC and for procedures that are necessary for creating the documentation. (9,10)

3. Qualification as per GAMP

GAMP 5: GAMP 5 guide offers A Risk-Based Approach to Compliant GxP Computerized Systems. It is set of guidelines designed by industry experts to help companies understand and meet cGMP regulation for computerized systems. This guide gives enough information on validation and compliance of computerized system throughout the life cycle. Most systems have components of varying complexity, such as an operating system, un-configured components, and Configured or custom components. Effort should be concentrated as follows: Custom > Configured > Non-Configured > Infrastructure**.** As per GAMP 5 systems are categorized based on the risk associated to commercial availability, configuration and customization. There are four different categories as per GAMP 5 based on system risk explained below:

- ➢ Category 1: Infrastructure Software

- Category 3: Nonconfigured products
- Category 4: Configured products
- Category 5: Custom applications

This is a natural evolution of this approach to software classification. So, we now have the above four categories. (11-12)

4. User Requirement Specification

The User Requirements Specification (URS) clearly and precisely states what the user wants the system to do, what attributes it should have and details any non-functional requirements and constraints. The following areas should be considered:

- Operational and data requirements
- Regulatory requirements including ERES
- Interfaces
- System access & security
- Data handling and reporting
- System capability
- Environmental health and safety
- Supplier support – documentation, testing

General requirements are linked to general characteristics and features expected from the information system and/ or to system hardware and software components. Regulatory requirements are the provisions set forth by the rules 21 CFR Part 11 & EU cGMP annex 11 and determined as applicable. Process requirements are directly linked to the processes managed by the computer system.

General Requirements: The following requirements are general purpose features requested for the system and are not related to specific business processes or regulatory issues:

Language: Interface language and manual language must be english

Instrument control: The system is able to control the instrument/equipment

Regulatory Requirements: This section identifies the regulatory requirements, determined by following regulations:

- US food & drug administration - code of federal regulations, title 21, part 11: “electronic records; electronic signatures; final rule”
- Guide to good manufacturing practice for medicinal products (the rules governing medicinal products in the European community, volume IV – annex 11).

The regulatory requirements are grouped according to the following regulatory Topics:

- Quality system: related to the quality system and to the associated documentation
- Security: related to the general features of system security and security of regulated electronic record managed by the system.
- Integrity: related to the integrity of the regulated electronic record managed by the system and associated Validation documentation. System GMP records must be protected from alteration/ deletion. If records can be altered by tools outside the system, the system shall detect and trace all the actions performed on records by pre-authorized operators (even at the highest level of access, such as system administrator).
- Traceability: related to the traceability of the regulated electronic record managed by the system.
- Accountability: related to the regulated electronic signatures managed by the system.
- Integrity Requirements: Data integrity/ altered record detection: System GMP records must be protected from alteration/ deletion. If records can be altered by tools outside the system, the system shall detect and trace all the actions performed on records by pre-authorized operators (even at the highest level of access, such as system administrator).

5. Quality System Requirements

These requirements are directly concerning the functionality expected from the information system and supporting the pharmaceutical company processes management.

Personnel training: All relevant personnel (i.e. process owner, system owner, qualified person, system developers and system administrators) should have appropriate documented qualifications in order to perform their assigned tasks

Risk management: Extent of validation and data integrity assurance should be based on a justified and documented risk assessment of the system.

Validation standards: The validation process for the computerized system should be defined according to pre-defined standards (e.g. policy, procedures) based on a justified risk assessment and should cover all the relevant steps of the system life-cycle.

System inventory: The computerized system shall be included in an up to date inventory listing all relevant systems and their GMP functionality.

System change control: Any changes to a computerized system including system configurations should only be made in a controlled manner and in accordance with a defined procedure. Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

Impact assessment document: The GxP impact assessment is carried out to determine if the computer system has an impact on product quality, patient safety or data integrity. All GxP impact computer systems must comply with applicable regulatory requirements.

Electronic Record and Electronic Signature Assessment: If an equipment/ system is determined as "GXP relevant" as per the GXP impact assessment, the following checklist is applicable (otherwise this checklist is to be skipped by answering all the question as "no")

Table 1. ERES Assessment Check Point

Sr.No.	Assessment Check Point	Yes/No
1	Does the equipment/ system create, modify, maintain, archive, retrieve or transmit electronic records specifically required by any GxP regulation?	
2	Are these records used in their electronic form to support GxP decisions?	
3	Does the equipment/ system support the application of electronic signature to records that are required by GxP regulation to be signed?	

- ❖ If all the questions are answered with "No" the equipment/ system is classified as "Non ERES relevant"
- ❖ If only 1 is answered with "Yes" the equipment/ system is classified as "Non ERES relevant"
- ❖ If 1 and 2 is answered with "Yes" the equipment/system is classified as "Electronic record (ER) relevant".
- ❖ If along with 1, 2 and 3 is also answered with "Yes" the equipment/system is classified as "Electronic Records (ER) and Electronic Signature (ES) Relevant".

21 CFR part 11 Assessment outcomes: Equipment/ system is assessed as (a) Non ERES Relevant (b) Electronic Records (ER) Relevant (c) Electronic Records (ER) and Electronic Signature (ES) Relevant. Depending upon the outcome of 21 CFR part 11 assessments, the validation requirement of the equipment/ system must be determined. Only if equipment/ system is determined as ER or ERES relevant, it should fall in the scope computer system validation. For equipment/ system, which is assessed as Non-ERES relevant qualification of the equipment/ system should be done in the same manner as for the other equipment/ system validation as per validation master plan. GAMP categorization should be used to decide on the amount of testing to be performed for the Equipment/ system qualification.

Table 2. GAMP Classification

Sr.No.	Question	Response (Yes/No)*	Category
1	Is the system infrastructure software e.g. operating system, database engine, programming language, statistical package, network monitoring tools etc.	□ Yes	The software is to be treated as GAMP category-1
		□ No	Go to question 2.
2	Is the system non-configured (run time parameter may be entered and stored but the software cannot be configured to suit business processes) e.g. firmware based application, COTS Software etc.	□ Yes	The software is to be treated as GAMP category-3
		□ No	Go to question 3
3	Is the system configurable (Software that can be configured by user to meet specific need of the user's business process however software code is not altered) e.g. LIMS, data acquisition systems, SCADA, ERP, BMS, EDMS etc.	□ Yes	The software is to be treated as GAMP category-4
		□ No	Go to question 4
4	Is the system custom designed and coded to suit the business process?	□ Yes	The software is to be treated as GAMP category-5.

* If tick Yes (✓) than software belongs to that particular category and if tick No (×) than software category considers as not applicable.

Configuration Specification: The Configuration Specification details the configuration parameters and how these settings address the requirements in the user requirement specification. This may be a standalone document or detailed in the functional specification.

System Description**:** Here we can write the system overview the installed application description and uses of application.

System Architecture: system is composed by the computer system and printer components.

System Specifications: In this chapter specifications covered by the system are described. The specifications are structured according to the following typologies:

- General Requirements Specifications: general characteristics and features expected from the system, independently from the specific process managed.
- Regulatory Requirements Specifications: requirements defined by the applicable regulations

- Process Requirements Specifications: directly related to the processes managed by the computer system.
- Functional Requirements Specifications: related to the single functionalities managed by the computer system. (This requirement should be defined only for high complexity system or system components/modules).
- Configuration Requirements Specifications: related to system Hardware and Software architecture and user's profiles /security settings and system settings..

6. Risk Analysis Document

Risk assessments should be performed at various key stages of the validation process by a multidisciplinary team so that a full understanding of all processes and requirements are covered and taken into account. This helps to identify and manage risks to patient safety, product quality and data integrity. An initial risk assessment is conducted early on in the project phase so that the results can be used in the validation plan, along with the outcome of activities in the concept phase, to define the depth and rigor of required activities and compile a list of deliverables. This produces a validation approach which is commensurate with the level of risk the system poses. A functional risk assessment is performed following approval of the functional specification to identify potential risks. Mitigation activities are then planned to manage the identified risks and allow focusing on critical areas, e.g.by modifying functionality, detailed testing, procedural controls or training. Further risk assessments can be performed during the course of the project such as testing and deployment, and for other activities throughout the life of the system. A risk assessment uses a simple scoring system documented in a matrix to produce the level of risk. A maximum scoring of 1 to 3 and low, medium and high are used to judge the severity of the risk, likelihood of occurrence and the probability of detection to attain an overall risk level

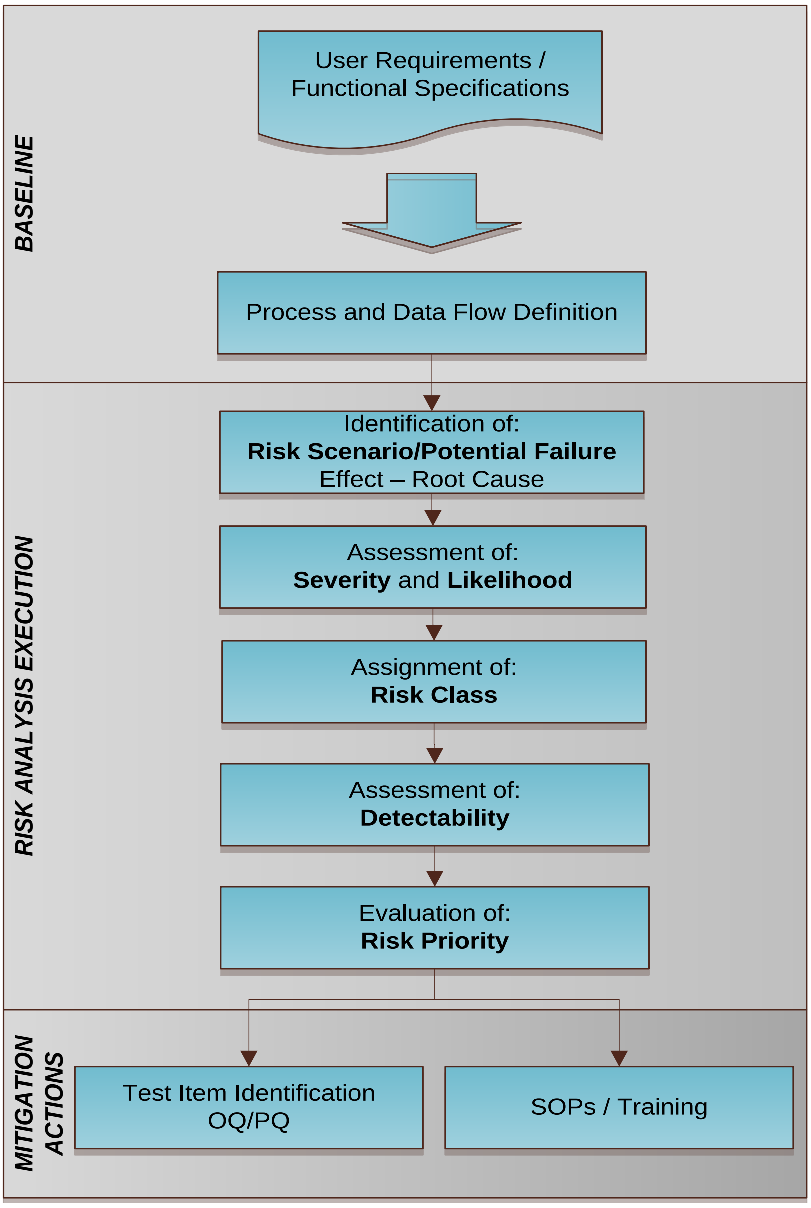
BASELINE
User Requirements / Functional Specifications
Process and Data Flow Definition
RISK ANALYSIS EXECUTION
Identification of: Risk Scenario/Potential Failure Effect – Root Cause
Assessment of: Severity and Likelihood
Assignment of: Risk Class
Assessment of: Detectability
Evaluation of: Risk Priority
MITIGATION ACTIONS
Test Item Identification OQ/PQ
SOPs / Training

Figure 1. Risk Analysis Procedure

Table 3. Severity of Effects

Severity	Criteria for Evaluation
High	The business process or function is used to create, update, or process data which may have direct impact upon either: • Product efficiency (i.e. quantity of active ingredient, potency if ingredients etc.) • Product integrity (contamination, cross contamination, storage and handling etc.) • Product Purity (i.e. recipe, use of ingredients) • Data integrity (i.e. data used to support a regulatory process or submission)
Medium	The business process or function is used to create, update or process data which have direct impact upon pharmaceutical quality attributes including: • Traceability (i.e. product routing, storage, materials movement, etc) • Status (i.e. quarantine, release, quality results etc) • Quantity (i.e. storage, packaging options etc)
Low	The business process or function used to create, update or process data which may have indirect impact upon pharmaceutical quality attributes or a direct impact on those functions that support cGxP operations such as: • Training records • Maintenance of system security settings or user profiles • Change control

Risk Class: The risk class for each risk scenario identified has been evaluated as a combination of the severity (Table 3) and of the likelihood (Table 4), as reported in the following table.

Table 4. Risk Class

		Likelihood		
		Low	**Medium**	**High**
Severity	**High**	**2**	**1**	**1**
	Medium	**3**	**2**	**1**
	Low	**3**	**3**	**2**

Where:

1 = High, 2 = Medium, 3 = Low

Project Validation Plan: The Validation Plan (VP) is produced to define the validation approach, describe the required activities, detail the acceptance criteria and list the deliverables and responsibilities. The VP specifies how flexible and scalable the validation approach will be which is derived from the outcome of activities in the concept phase.

7. Validation Approach

The validation strategy is risk-based. It considers the following:

- Potential impact to quality, efficacy and safety of a drug product.
- Potential impact on the integrity of data used to support drug safety and regulatory submissions.
- Size and complexity of the computerized system.
- Standardization of the software and hardware components being used.
- Scope of Vendor involvement.
- Quality and extent of the Vendor document.

The validation strategy will ensure that: The validation is a part of the implementation process. The validation meets the requirements of the Computer Systems Validation standard operating procedure. A formal system management procedure is in place for the management and operation of the installations. The validation strategy is risk-based. It considers the following:

- Potential impact to quality, efficacy and safety of a drug product.
- Potential impact on the integrity of data used to support drug safety and regulatory submissions.
- Size and complexity of the computerized system.
- Standardization of the software and hardware components being used.
- Scope of Vendor involvement.
- Quality and extent of the Vendor document.
- GxP Relevant
- Electronic Record Relevant

- Electronic Signature non-relevant

Installation Qualification: The Installation Qualification (IQ) is the documented proof that components have been delivered, installed and configured in accordance with the requirements and statutory safety regulations stipulated in the specification documents. The system is delivered by the vendor with document software and therefore the installation qualification of vendor qualification document covers the qualification of computerized component too.

Operational Qualification: The Operational Qualification (OQ) is a test process that evaluates the correct functioning of the computerized components of the system. It will also cover the identification and inspection of alarm, control and switch functions that have influence on quality. During the Operational Qualification, all items specified in the test plans are processed and documented in writing, to ensure that the system function in accordance with the specifications. A successful Operational Qualification without any major or critical discrepancy indicates that the system can be accepted technically. The operation of the system is controlled by the software. The operational qualification done at the system level and that the validation of the computerized system is done in conjunction with the qualification of the vendor qualification document.

Performance Qualification: The purpose of performance qualification is to verify and document that the system is working reproducibly with the entire specified working range and limits. The performance qualification also aims at ensuring that the system operates as intended in a secure and reliable way in alignment with the analysis activity. Since the performance of the computerized components of the system has a key role in the performance of the equipment, the performance qualification will be performed in conjunction with the equipment qualification. (13-16)

Reporting Phase: This section covers how the system will be released for the production use. The system will be released for production use, subject to complying with the quality standards defined in the validation plan and on meeting the qualification expected result.

Validation Report: A Validation Report will be issued when Operational and performance qualifications of the system are successfully performed, without any major or critical observation and when all the planned activities defined in the project validation plan are completed. It will also be ensured that all other activities that are required to be completed as per this PVP and equipment qualification are done, and deliverables are made available. The system is considered to be released as soon as the validation report is signed. Therefore, a separate System Release Notification will be issued. The acceptance criteria that will be considered on system release are described separately under sub-section “Acceptance Criteria” below.

Acceptance Criteria: An installation will be considered as validated and released for the operation use on meeting the following requirements:

- All the activities, according to the plan, are performed and a confirmation and evidence to this effect is available.
- The life cycle documents, as applicable, are available with approvals.
- Test results are evaluated and ensured that major and critical deviations are retested and closed.
- Traceability among the document items is assured.
- The training materials, training plan, training records, user manuals are available.
- The relevant standard operating procedures are updated and published.
- System management procedures, as applicable, are implemented and followed.

Vendor Assessment is completed, and the lapses are documented with responsibility and target completion date.

Operation phase:

System Management: While the management of the equipment is handled by the respective Standard Operating Procedures, the management of the computerized components in the system will be handled as per the details given below:

Change Management: Changes during the operation phase will be handled as per the current change control SOP.

User account Management: System access will be granted in accordance with the existing Access Control and Password Management Standard Operating Procedure.

Backup management and restoration: The backup operation of the system will be handled as per the Standard Operating Procedure; the restoration of the backup will be handled as per the Standard Operating Procedure.

Non-Conformation Management: The Non-confirmation activity and the related deviations related to the system will be handled as per the Standard Operating Procedure.

Corrective and Preventive Action (CAPA): The incidents that falls within the scope of Corrective and Preventive actions will be handled as per the Standard Operating Procedure.

Periodic Review: The validation status of the system will be reviewed at least every three years from the date of approval of the system and release to production use, as per the validation plan.

Retirement: Whenever an installation is required to be retired, a system retirement plan will be prepared in order to ensure the orderly transfer of operations to new application software, or otherwise, and to ensure the archival of data. The retirement of the system will be done as per the validation master plan.

Requirements traceability matrix document: The purpose of this document is to provide a traceability matrix for the qualification of requirement specification. the trace matrix (tm) maps the approved user requirements to associated configuration specifications document (CSD) and includes the test script in order to verify that each requirement has been successfully tested. the tm is to be reviewed and approved as part of the approval process of the qualification/validation report.

Qualification summary report: This document is prepared to summarize the validation activities of system performed as per validation plan. This document is also prepared to establish documented evidence that, the system meets the requirements defined in the user requirements specification (URS) document.

Adoption of System Life Cycle Documents: During the project, a few of the life cycle document items like the user manual etc. will be provided by the vendor in their own template. At times, a document of another site also may be used to fulfil the validation requirement. E.g. Impact Assessment Document. The system owner and the process owner or their assignees will review these documents and conclude whether the documents can be accepted conditionally or unconditionally.

Document Version Control during project: Any changes in the version of system life cycle document until the release of the validation report will be handled by updating the version and version history within the document.

Storage of Documents: The system life cycle documentations will be handled by the external/internal consultant supporting the validation during the implementation of the system. These documents will be handed over to the the respective documentation department after the release of the system for production use. Thereafter, the system owner will continue to be the owner of the documents, irrespective of whether the documents are in his/her custody or not.

8. Conclusion

This paper discusses the regulations for computerised systems and discusses some of the practical options available for qualification and risk assessment for computerised system validation (CSV). Successful regulatory inspections are more crucial for survival of any pharmaceutical company. Success of inspections purely depends on quality and integrity of data provided to auditors during inspections. Data integrity is essential tool to offer adequate confidence to regulatory bodies on data associated to manufacturing and testing process at each pharmaceutical firm. Computer system validation and qualification of equipment is an important tool to establish and maintain data integrity controls though out the data life cycle. Computer system validation approach of pharmaceutical manufacture should be implemented in line with GAMP 5 guideline to confirm 21 CFR Part 11 and other major regulatory compliance.

Acknowledgements

Authors are thankful to Department of Science, Shri Satya Sai University of Technology and Medical Sciences Sehore and quality assurance department Alembic pharmaceutical limited, Vadodara for providing the necessary facilities & guidance to carry out this industrial research and wrote paper.

Financial Disclosure statement: The author received no specific funding for this work.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

1. U.S. Food and Drug Administration, Pharmaceutical cGMPs for the 21st Century: A Risk-Based Approach; 2002.
2. U.S. Food and Drug Administration, Guidance for Industry: 21 CFR Part 11; Electronic Records. Electronic Signatures Part 11 Scope and Application; 2003.
3. International Standards Organization, ISO Standard 14971 - Medical Devices - Application of Risk Management to Medical Devices, International Standards Organization, Geneva; 2000.
4. Guidance on equipment qualification of analytical instruments, Accreditation and Quality Assurance. 1996; 1(6):265-74.
5. Coombes P, Laboratory Systems Validation Testing and Practice, DHI Publishing, LTD, Raleigh, USA; 2002.
6. US Food & Drug Administration - Guidance for Industry Quality Systems Approach to Pharmaceutical Current Good Manufacturing Practice Regulations; Sept 2006.
7. GAMP Forum – GAMP Good Practice Guide, A Risk-Based Approach to Operation of GxP Computerized Systems; 2010.
8. US Food & Drug Administration - Guidance for Industry Process Validation: General Principles and Practices – Revision 1; Jan 2011.
9. US Food & Drug Administration - General Principles of Software Validation; Final Guidance for Industry and FDA Staff; Jan 2002.
10. PIC/S Good Practices for computerized systems in regulated "GxP" environment, Pharmaceutical Inspection Co-operation Scheme guidance; Sept 2007.
11. GAMP Forum – GAMP Guide, A Risk-Based Approach to complaint GxP Computerized Systems - Ver. 5.0.
12. GAMP Forum – GAMP Good Practice Guide, Global Information Systems Control and Compliance.
13. Society of Quality Assurance, Computer Validation Initiative Committee (CVIC), Risk Assessment /Validation Priority Setting.
14. GAMP Forum, Good Practice Guide - IT Infrastructure Control and Compliance, International Society for Pharmaceutical Engineering, Tampa, FL; 2005.
15. McDowall R. D.In Computer Systems Validation: Quality Assurance, Risk Management and Regulatory Compliance for Pharmaceutical and Healthcare Companies, Interpharm / CRC, Boca Raton, FL; 2004.
16. Agalloco, J, Carleton FJ. Validation of Pharmaceutical Process. 3rd Edition. USA, New York: Informa Healthcare; 2008.