IJBPAS, November, 2022, 11(11): 5256-5266

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

COMPUTERIZED SYSTEM VALIDATION – A REVIEW

SAVITHA S[1*] AND KATHIRESAN K[2]

1: PG Student, Department of Pharmacy, Annamalai University, Chidambaram, Cuddalore, Tamilnadu, 608002

2: Associate Professor, Department of Pharmacy, Annamalai University, Chidambaram, Cuddalore, Tamilnadu, 608002

***Corresponding Author: S. Savitha: E Mail: savithaoreo55@gmail.com**

Received 26th Dec. 2021; Revised 24th Jan. 2022; Accepted 14th Feb. 2022; Available online 1st Nov. 2022

https://doi.org/10.31032/IJBPAS/2022/11.11.6567

ABSTRACT

In the pharmaceutical industry, computers are an integral part of day-to-day operations. In the last 20 years, data administration in the GMP area has transitioned from paper-based approaches to computerized solutions. We use an established, effective, and controlled computer system to improve the integrity of our quality assurance system. Software issues can have a negative impact on environmental production and result in a drop in product quality. Validation assessment is required in the pharmaceutical industry to assure compliance with medication cGMP criteria and consistent quality.

Keywords: Computer System Validation, Life cycle model, Requirements of Regulated Electronic Records, Qualification of CSV

INTRODUCTION

Computers are used to create and develop medical gadgets and medications. The functionality and performance of software and computer systems are critical in establishing data stability, confidence, security, and correctness. It is critical to use computer systems to reduce product identification, purity, strength, and efficiency by ensuring uniform and secure procedures and reducing human error.

Defects, failures, and errors in computerized systems must be identified from time to time throughout the computer system validation process. As a result, the US Food and Drug Administration considers computer systems to be equipment under 21 CFR 211.68 (FDA). For production and quality control, computerized control has increased considerably in recent decades. FDA has published software validation recommendations. In addition, the GAMP (Good Automated Manufacturing Practice) guideline was adopted as a norm in most computer system validations **[1]**.

Computerized system: A computer system controls the performance of one or more automated processes as a whole. Hardware, software, peripherals, networks, personnel, and documentation are all part of the package (e.g. manuals and sop).

Computerized system validation: By examining and providing objective evidence, computerized system validation ensures that the computerized system (hardware and software) specifications conform to the User's needs and intended use, and that all criteria can be met consistently **[2]**.

GAMP (GOOD AUTOMATED MANUFACTURING PRACTICE)

Good Manufacturing Practices (GMPs) were established in 1991. It is the current edition of the GAMP 5 and establishes guidelines for producers. ISPE establishes standards for manufacturers. GAMP provides a number of policies and procedures that must be followed to ensure that pharmaceutical software meets the highest standards. In order to comprehend the validation process obligations, users and suppliers of computer system validation should work together to fulfill cGMP criteria **[3]**.

21 CFR PART11

The FDA rule establishes the 21 CFR PART 11 which applies to electronic signatures and electronic records generated, edited, held, archived, retrieved, or communicated by anyone in any record described in the Federal Food, Drug, and Cosmetic Act, Public Health Service Act, or FDA regulations. Appendix 11 of the European GMP guidelines contains reference specifications for computer systems used by enterprises in the pharmaceutical industry **[4]**.

LIFE CYCLE MODEL

A life cycle model is used in the development of software systems. In the software system development technique, each phase is linked to a computer validation step. As a result, this model may be used to show each phase of the validation process in

computer system validation. This makes it possible to effectively document the development process. The model's description by Augsburg *et al*. is provided (1994). The life cycle model is depicted in **Figure 1** as a series of basic steps.

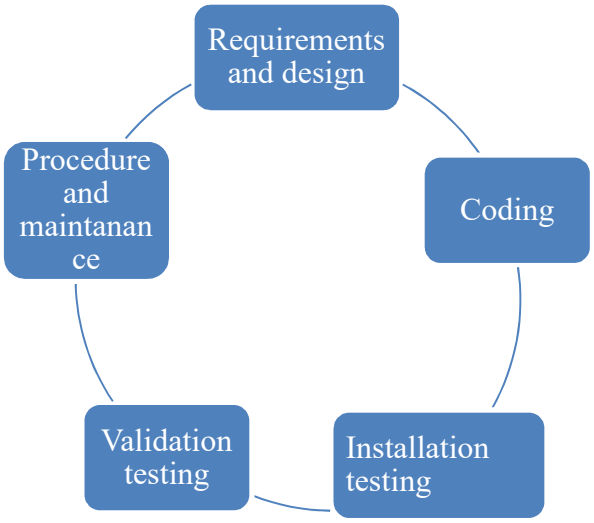

Figure 1: Life cycle Model

Step for this model is given below:

Requirements for design:

A new computerized system must be capable of replacing or restarting an existing pharmaceutical process. When the life cycle begins, the group of people who will be in charge of validation should be chosen. The validation plan must be created before the resources to be validated can be determined. The finished computerized system must be documented and explained in detail. The documents that will be prepared will be identified during the validation. The system documentation, which included procedures and reporting, may be modified as a result of validation activities.

Coding:

The validation plan may be completed at the beginning of this phase. Everything could be clarified about the validation test environment, assumptions, system exclusions, limits and installation methods. This step involves software and hardware installation.

Testing:

This process is divided into several stages. For each individual module, either the hardware or the software should be tested. After that, an integration test is required. "If developers perform unit, system, and integration testing, the validation committee will be able to define

test cases for data running on the acceptance test".

Installation testing:

End users test the system using their own data and methods. The system's failure necessitates re-design and documentation.

Production system maintenance:

The production system is turned on. System modifications (whether software or hardware) must be documented and regulated in advance. The performance function is linked to stage five of the above-mentioned lifecycle model, and steps three and four will be verified in installations. Design qualification will be addressed in the first and second step **[5, 6]**.

V-MODEL

The GAMP organization for good automated manufacturing practice has issued guidelines for pharmaceutical sector suppliers. With the advent of the computerized production process, a somewhat different model is used as primary direction. Boehm's V-model is depicted in **Figure 2** (Boehm, 1979). Each level of the V-model corresponds to one model life-cycle step **[7]**.

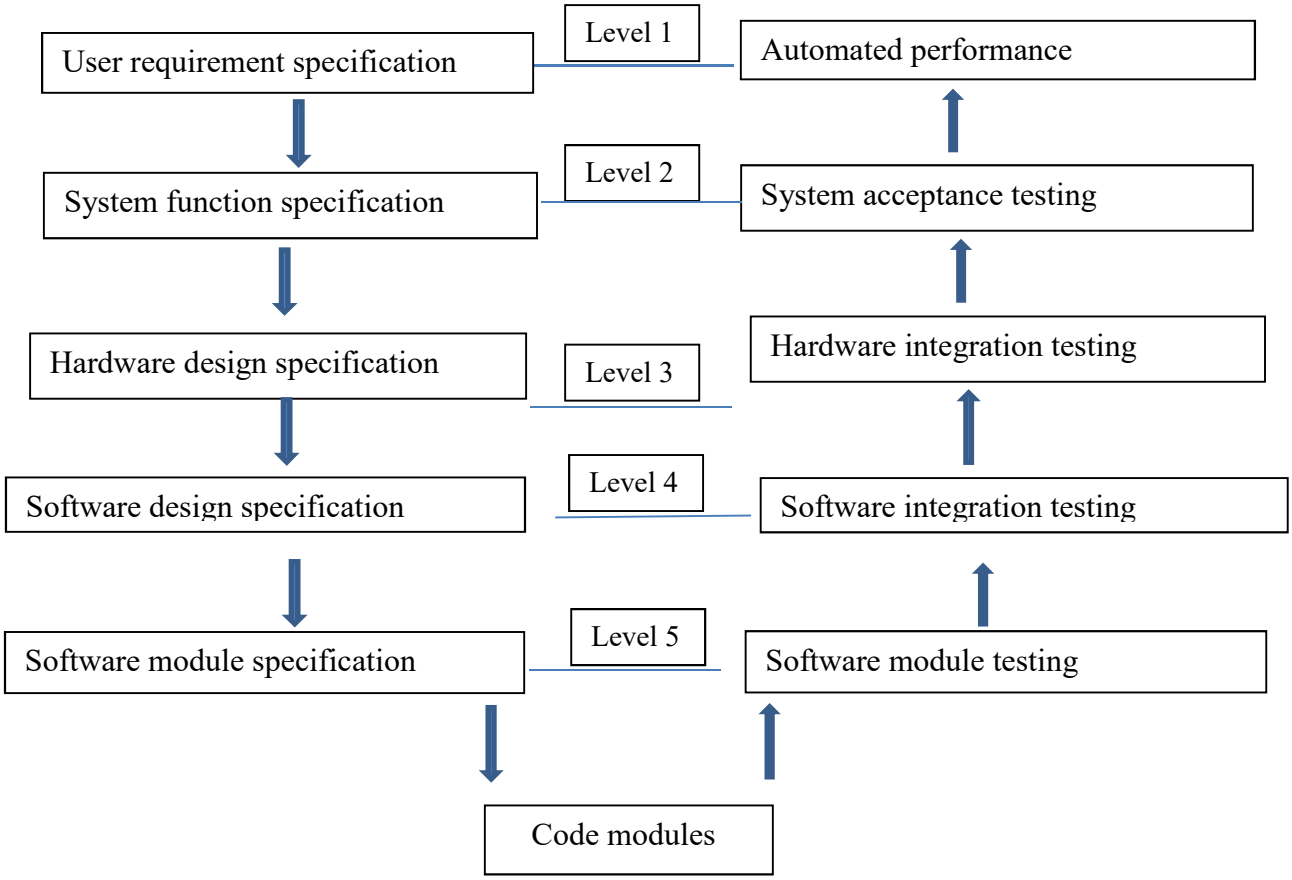

Figure 2: V-Model

REQUIREMENTS FOR REGULATED ELECTRONIC RECORDS

Organizations employ a range of computerized systems to handle regulated electronic records in order to facilitate a large number of operational operations, including those developed and depended on to ensure patient safety and product quality. Each regulated organization is responsible for the complete examination and monitoring of all computer systems and their management in line with GMP regulations. Companies must understand the nature and scope of computerized systems, and evaluations will be conducted with the goal of describing each system, its intended purpose and function, as well as any risk or vulnerability to data integrity manipulation.

Computer System Validation

Computerized system validation (CSV) is a documented process that entails the adoption and application of policies, methodologies, and life cycle measurements in validation plans and reports in order to assure compliance and maintenance with respect to the applicable GMP regulatory rules and fitness. Validation activities ensure that the system environment implements and maintains configuration and design control settings for data integration throughout the system's lifecycle (including the software application and operating systems environments).

- Where technically possible, limiting system administrator security settings to independent personnel.
- Configuration settings that allow data to be rewritten and reprocessed without being traced should be disabled.
- Implementing a time/date stamp and limiting access **[8]**.

DATA ENTRY/ CAPTURE

Systems are built to accurately gather data that is collected manually or automatically.

For Manual Entry:-

- Only authorized individuals can manually enter data, and the system will record the entry details, including who entered and when the entry was made.
- Data is entered in a software-controlled, pre-defined format, with confirmation to guarantee the system does not accept invalid data forms.
- Even if submitted data has an impact on product quality and safety, any manual data entries must be verified by a second operator using validated computerized techniques.

For automated data capture:

- The interface between the source system, acquisition system, and recording system is tested to guarantee that the data is correct.
- The software shall attach a verified check to confirm the completeness of acquired data and any metadata connected with the data.
- In order to confirm the completeness of acquired data and any metadata associated with the data, the software shall attach a validated check.
- Required data modifications should be approved and monitored in accordance with established procedures. For example, manual integration and rework of laboratory results must be approved and controlled. The company's Quality Unit must take steps to ensure that data modifications are performed only by authorized personnel when necessary **[9]**.

SECURITY

1. System Access

In order to prevent unauthorized access, modification, or deletion of data, user access controls are established and applied both physically and electronically. Personal login IDs and passwords will be provided to all employees who need to access and use the specified electronic system. Sharing login credentials makes it impossible to identify the individual who is executing the activity; thus, password sharing should be prohibited (even though justified on account of financial savings).

2. Backup

The Backup and Recovery Processes outline the backup and restoration actions that are necessary. Backup and recovery processes are evaluated to ensure complete recovery capabilities and metadata in the event of a failure. To ensure proper operation, a backup verification mechanism (automatic or manual) will be in place. Backup and retrieval processes (e.g., process addressed) are recorded, validated, and monitored on a regular basis. Each backup is double-checked to verify that it works properly. Regular backup copies (i.e. media where backup data is saved) will be stored in a remote place in the case of a disaster (physically separated).

3. Data Migration Verification

The process of transferring data and information between storage medium or computerized systems is known as data transfer/migration. When necessary, data migration might change the data format so

that it can be displayed or used on a different computer system.

The data transfer/migration methods go through a streamlining process and are thoroughly created and tested to ensure data integrity throughout its lifecycle **[10]**.

TRACEABILITY

1. Audit Trail

The audit trail, which is a type of metadata that contains information on the creation, change, or deletion of the electronic registration regulated, is automatically recorded by the system. A trail of the Audit allows for the safe recording of life-cycle details such as creation, addition, deletion, and alteration without obscuring or overwriting. An audit trail aids in the reconstruction of the history of such events, regardless of the materials involved, including who, what, when, and why.

The following information should be included in audit track records in a readable format:

- The name of the person who made the change in the data;
- Interpretation of change
- Time and date of change
- Reason for change **[11]**.

INSPECTABILITY

1. Electronic Copies

Inspectors can use the PC to create accurate and complete inspection, review, and copy records in both human readable and electronic formats.

2. Archiving

Data shall be archived on a regular basis using defined procedures. The backup data, which is stored in a different and remote place, is physically protected from the archived copies. During the archiving time, the data will be available and easy to read while maintaining its integrity.

ACCOUNTABILITY

1. Electronic signature

Electronic signatures must have proper control in order to guarantee the authenticity and traceability of the records to a specific individual who electronically signed them. The use of electronic signatures shall be regulated effectively, taking into account:

- ✓ How an individual's signature should be formed.
- ✓ How the signing procedure is documented on the system so that the signature or status of the entry is either invalidated or manipulated.
- ✓ How the signature record is related to the entry and can be validated.
- ✓ Electronic signature security, i.e. only the signature's owner can use it.

The system signing procedure is supposed to be validated in order to show its sufficiency and maintain control over the signed records. The electronic signature information is kept with the document when a paper or PDF copy of the signed electronically is printed. Electronic signatures or electronic signature systems are required to give the signature manifestation, which is the record that defines the signatories, the associated function (where possible), the date (and time, if applicable), and the meaning of the signature (e.g. verified or approved) **[12]**.

HOW THE VARIOUS STAGES IN THE COMPUTER SYSTEM VALIDATION ARE PERFORMED?

There are several stages to the computer system validation:

- ✓ Determine the parties' roles for the various aspects of the project.
- ✓ A description of the tool, system, processes, and testing procedures to be performed.
- ✓ Determining acceptance criteria for each system is a procedure that must be validated.
- ✓ All SOPs have been established.

User Requirement Specification

- ✓ System needs and process control are determined.
- ✓ Establishing a common programming and testing procedure.
- ✓ Project responsibility and timelines are assigned to integrated groups.
- ✓ Provide adequate specifications to the supplier to estimate cost, resources, and time for creating and documenting the system in a validation life-cycle **[13]**.

Installation Qualification

The I.Q Protocol contains instructions for installing and verifying hardware and software components. All elements of the protocol are verified, dated, and signed by this operator. During an I.Q. test, the following items are frequently tested.

- ✓ Electricity, power supply and connection
- ✓ Uninterruptible power supply and emergency power supply
- ✓ Grounding termination and tagging
- ✓ Control boxes and environmental conditions
- ✓ Equipment codes and identification tags
- ✓ Device tube and writing continuity

- ✓ Drawing (P and ID, loop sheet, wiring plan and termination, network plans)
- ✓ Purchase order
- ✓ Manuals

Operational Qualification

The O.Q test checks the system's operation as well as the I.Q protocol's approval. It entails both static and dynamic testing to guarantee that all continuous, sequential control and graphical displayed component activities are accurately tested and documented. The following items should be evaluated:

- ✓ Signal range testing
- ✓ Alarm points and priorities
- ✓ Network communication
- ✓ Security system
- ✓ Signal and integrated sequence
- ✓ Report and data achieve format

Performance qualification

Multiple (traditionally at least three) production procedures are used to qualify performance, with representative batch sizes for the activity. These should be performed with a pharmaceutical product and the computer and manufacturing services system outlined in SOPs and URS for the plant Computer system performance qualification tests include combining IQ and OQ tests to ensure that the computer system, when combined with plant equipment and procedures, can function precisely and reliably according to the specification. Its primary goal is to demonstrate how the system monitors, monitors, and records essential parameters, data, and functions, as well as how efficiently and consistently the systems can be loaded and processed under varied scenarios. For PQ testing

OQ test methodologies may be used as-is. Tests should be made, such as critical parameters, directly linked to data integrity and system repeatability.

- ✓ System access security
- ✓ Operator interfaces
- ✓ Software installation verification
- ✓ Control and monitoring loop function
- ✓ Alarm, event and message handling
- ✓ Safety and operational interlocks
- ✓ Verification of SOP
- ✓ Data records and reports
- ✓ Power loss and recovery **[14, 15]**

CONCLUSION

For successful computer system validation, quality management and the formal life cycle model and qualification completed throughout the life cycle model are extremely important. The CSV must guarantee that the system meets all criteria

and user expectations. Both operational controls are maintained daily and efficiently to preserve the validation status of a computerized system. The computer system validation process is supported by fundamental principles such as the life cycle model and the V-model. The Computer System Validation (CSV) framework for the present validation process might help future implementers significantly improve the validation scope, saving time and effort for manufacturers.

REFERENCE

[1] Ludwig Huber, Analytical Instrument Qualification and System Validation. Agilent Technologies, 2009, Publication Number 5990-3288EN.

[2] WHO Good Manufacturing Practices for Computerized System Validation WHO Technical Report Series, NO. 937, 2018, Annex 5.

[3] GAMP Forum - GAMP Good Practice Guide, Global Information Systems Control and Compliance.

[4] Code of Federal Regulations 21, Parts 11 (August, 1997), 210, and 211.

[5] Andreas Hoffmann, Jacqueline, Marcel Plattner, Vanja Schmidii-Vckovski, Christian Kronseder. "Computer System Validation: An Overview of official requirements and standards". Pharmaceutics Acta Helvetiae, 1998.

[6] Nash R. A., Wacher A. H., Pharmaceutical Process Validation, An International 3rd Edition, Revised and Expanded, Marcel Dekker, New York, March.,2003; 31-57.

[7] CFR, 21 CFR, Part 211: Current Good Manufacturing Practice for Finished Pharmaceuticals, sections 21I 22: Proposed Rules, vol. 61.Federal Register, pp., 1996; 20104-20115.

[8] GAMP Forum – GAMP Good Practice Guide, A Risk Based Approach to Compliant Electronic Records and Signature.

[9] GAMP 5- A Risk Based Approach to Compliant GxP Computerized Systems ISPE, 2008.

[10] Data Integrity and Computer System Validation by Federal State Institute of Drugs and Good Practices with PQE group

[11] European Commission: Annex 11 "*Computerized Systems*" to the EU Guidelines of Good Manufacturing Practice for Medicinal Products.

[12] Sharon Strause - Computer System Validation - Definition and Requirements, Originally published in

the spring 2009 issue of Journal of Validation Technology, pp-1-5.

[13] Lopez, O., Qualification of Computer Networks, 1st ed. Storrington, West Sussex, UK Sue Horwood Publishing Limited, 2000. ISBN 1-904282-00-8.

[14] Potdar M.A, cGMP for Pharmaceuticals, Pharmaceutical Validation, 3rd Edition, Nirali Prakashan, Pune, 437-450.

[15] Ostrove, S.: Qualification and Change control, IN: Validation of Pharmaceutical Processes, 3rd Edition: Agalloco J. Carlton, F. New York: In forma Healthcare USA, Inc., 2008.