**Document approval**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Date** | **Signature** |
| **Author’s designation**  **e.g., Quality Specialist** |  |  |  |
| **Reviewer’s designation**  **e.g., Quality Management Director Deputy** |  |  |  |
| **Approver’s designation**  **e.g., Quality Management Director** |  |  |  |

|  |  |
| --- | --- |
| **Effective Date** | **2023-01-28** |

**Table of Contents**

[1 Purpose 2](#_Toc95307591)

[2 Scope 2](#_Toc95307592)

[3 Responsibilities 2](#_Toc95307593)

[4 Definitions, terms and abbreviations 2](#_Toc95307594)

[5 Workflow 3](#_Toc95307595)

[6 Applicable documents 3](#_Toc95307596)

[7 Appendices 3](#_Toc95307597)

[8 Document revision history 3](#_Toc95307598)

# Purpose

The purpose of this Standard Operating Procedure (SOP) is to provide guidance on the requirements to a risk-based approach on how to handle computerized systems.

# Scope

This SOP is valid at Company ABC for all Organization. The respective training shall be given in accordance with **SOP-10 Training Management**.

All GXP computerized systems are covered by this SOP. Any systems (e.g., control modules) that are needed to effectively control an instrument or equipment to be functionable are out-of-scope.

In case of analytical equipment software an integrated approach may be used and incorporated in the initial qualification and/or validation efforts.

# Responsibilities

Responsible for the content of this SOP is e.g., Electronic Data Manager.

|  |  |
| --- | --- |
| **Role** | **Definition/Task** |
| Quality Organization | * is responsible to ensure adherence to the document and compliance with the regulations. |
| e.g., Quality Management Director | * Is sign off the respective documents and provides guidance as outlined herein |
| e.g., Regulatory Affairs Head | * ensures compliance with potential filings. |
| e.g., Manufacturing Head | * ensures that only validated systems are used for the manufacture of GxP materials. |
| e.g., QC Head | * ensures that all system interfaces of analytical equipment, (e.g. into a laboratory information management system) follow this procedure. |
| e.g., Electronic Data Manager | * responsible for all systems that are not integral part of the system controls of an equipment or machine. |

# Definitions, terms and abbreviations

|  |  |
| --- | --- |
| **Term/abbreviation** | **Definition at Company ABC** |
| CSV | Computerized System Validation |
| GAMP | Good Automated Manufacturing Practice |
| IQ | Installation Qualification |
| OQ | Operational Qualification |
| PQ | Performance Qualification |
| SMART | Specific, Measurable, Attributable, Relevant, Time-bound |
| URS | User Requirement Specification |

# Workflow

## System Requirements Identification

User Requirements Specification (URS) for computerized systems are written in non-technical language that is testable and measurable and cover the user’s point of view. The requirements follow the SMAR(T) rule.

The user requirements address the following, where applicable:

* standards, regulatory, and legal requirements (e.g., Security, GxP);
* Data Integrity (including data flow and data lifecycle requirements);
* Constraints (e.g., downtime limitations);
* Precision, accuracy, and format for records and metadata;
* Identification of electronic records and signatures;
* Interface and infrastructure requirements;
* Backup, restore, and disaster recovery requirements;

The requestor requests and initiates Change according to **SOP-05 Change Management.**

The requestor documents the requirements in the URS, which is approved by e.g., Quality Management Director. URS must be approved prior to test protocol/specification approval, and must be maintained throughout the life cycle of the system, during project and after release.

## Risk Assessment

The business, technical and quality groups determine Risk classification of system and generate the risk assessment, according to **SOP-09 Quality Risk Management**.

Risk classification is based on software complexity, innovation, and the level of configuration and customization that will be required. Software categorization is a key lever in determining the required Computerized System Validation (CSV) results and is the basis for making other risk-based decisions.

Good Automatization Practices (GAMP) categories (which define software complexity) include:

* GAMP Category 1 Software – Infrastructure (e.g. Operating Systems),
* GAMP Category 2 Software – Instruments and Controllers,
* GAMP Category 3 Software – Non configured software (e.g. established packages allowing set-points),
* GAMP Category 4 Software – Configured software, and
* GAMP Category 5 Software – Customized software.

## Periodic Review

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

The validation status of each GxP electronic system should be reviewed at least every three years. The periodic review should be initiated by the process owner or system owner and should be documented, reviewed by the business process owner, and approved the system owner and, in GMP areas, the approval is done by Quality Organization.

The periodic review report should either conclude that the system is usable or justify why continued use is acceptable while unsatisfactory issues are resolved or should recommend termination of the system during remediation. If gaps affecting compliance have been identified, a Corrective And Preventive Action (CAPA) plan should be developed to correct them in a timeframe consistent with the identified risks. Upon completion of the periodic review, the system's register document should be updated accordingly.

## Documentation:

All computer system conformance documentation should be reviewed, including vendor documentation created specifically to support the development, implementation, validation or management of individual systems. It specifically excludes internal vendor documentation that are not written specifically for the customer.

**SOP-02 Good Documentation Practice** is to be followed.

## Training

Electronic systems must be designed, operated, maintained and managed by qualified personnel. This means that people (both employees and contractors) need a combination of training, education and experience that will enable them to fulfil their assigned responsibilities. Procedures shall be established to maintain documentary evidence (e.g., training records) to indicate that all individuals involved in computer system compliance have received sufficient training required to perform their assigned duties. This training should include users, system and process owners, and support personnel such as IT and engineering staff.

**SOP-10 Training Management** is to be followed.

## Validation Planning

A validation plan (or qualification plan if the system is not used in a validation setting) is required for projects that introduce new GxP electronic systems and for major changes to existing GxP electronic systems. The methods allowed are discussed on a case-by-case basis. Similar systems may be tested in the same plan, provided that all features (general and specific) are detailed in the plan.

The validation plan shall determine the approach to establishing and maintaining the validated status of the computerized system and ensure that all validation efforts are managed. The Department head of the process owner and Quality Organization review and approve the validation plan prior to the start of any assessment activity.

At a high level, validation plan includes:

* An overview of a computer system and a description of the system, including interfaces and system boundaries.
* Definition of applicable **MD-01 ABC Quality Manual ABC** requirements, policies, procedures, and industry standards.
* Overall validation strategy (including detailed life cycle and data life cycle, distinction between GxP and non-GxP functions with the linkage to all appropriate certifications and documents).
* Quality Risk Management activities, including the results of applicable risk assessments
* GAMP software category assigned
* Identification of the required CSV lifecycle deliverables
* Use of vendor resources and/or documentation (including outsourcing and use of any service models, such as software as a service).
* The vendor documentation to be used must be evaluated for suitability, accuracy and completeness.
* Test strategy and approach, handling of test defects
* Acceptance Criteria and System Release Strategy
* Roles and responsibilities
* Required end-user outcomes (training, SOPs, etc.)
* Procedures and plans required to maintain a validated status
* File storage and management information (location, procedure, etc.)

## Specifications

Specifications are covered in the URS addressing all requirements regarding stakeholders. Additional items cover all functional specifications/parameters, and any type of particular configuration and design requirements. While the project is ongoing the document may reflect this. The final version is to be approved Quality Organization prior to acceptance.

The URS is the basis for all further qualifications efforts and will be checked against when completing the Performance Qualification/validation.

For software of-the-shelf or customized by the software provider, the functional and design responsibility is with the software provider.

## Installation Qualification (IQ)

In order to complete the IQ, one should get (either separate or combined):

* supplier records for executed installation,
* log-file verifying successful installation, and
* report all configurations are met as outlined upfront

Ensure that a Risk Assessment according to **SOP-09 Quality Risk Management** covers all respective items to ensure configuration errors are covered in an automated infrastructure (e.g., cloud based solutions). Infrastructure includes servers, networks, datacenters, computers, and the associated operating systems.

## Operational Qualification (OQ)/ Functionality Testing

Aim of the OQ is to demonstrate that the system works as intended. Within the OQ a test plan should be written and executed to ensure:

* Roles and Responsibilities can be set-up.
* Test environment description are covered (if there is no test environment, use a risk-based approach and mitigate any potential negative impact on the live-system).
* Documentation for recording analysis and defects are set-up.

In order to check all functions, a test script/specification is outlined. It includes (but are not limited to):

* Clear identifiers of the software, version and release date
* Test steps
* Expected results
* Actual Results along with a pass/fail check-box.

The test protocol and the specification have to be approved upfront and ensure traceability to each other.

The test execution is recorded as outlined. All deviations from the predefined specifications are recorded, evaluated against their impact on the (GXP) requirements and resolved where required according to **SOP-06 Deviation and Nonconformance Management.** The defect list is part of the final report.

All information from the test scripts along with the specifications and defect lists, along with all other relevant information are concluded in a final report. The report must state if the final assessment is deemed successful or not. Any items that remain open should be converted to a CAPA to ensure follow- up actions and traceability.

Learnings and results from performing the OQ should be processed into work instructions and SOPs.

## Performance Qualification (PQ) /User Acceptance Testing

During the test the system should be challenged, and the robustness confirmed. The approach is comparable to the OQ set-up but needs to clearly outline the items to be challenged.

The traceability to the URS needs to be ensured and established. Procedures (SOPs, WI) need to be tested for suitability and robustness. If the system tests were performed, the starting of system operation needs to be documented and requires strong surveillance in the beginning of using the new system in the live environment.

## Changes and Configurations Management

Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with **SOP-05 Change Management**.

## Security

Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. Creation, change, and cancellation of access authorizations should be recorded.

Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

## Retirement Phase

At the end of the lifecycle the system will be formally retired. A retirement plan will be developed and approved by all stakeholders to insure minimal risk to the ongoing operations. The plan needs to include:

* Back-up plan and archiving of files along with a strategy on how to handle native files,
* Impact Assessment (e.g., interfaces, system integration issues),
* Change initiation (according to **SOP-05 Change Management**),
* Updating all system lists and schedules,
* Decommissioning of equipment as applicable.

# Applicable documents

MD-01 ABC Quality Manual ABC

SOP-01 Documentation Management

SOP-02 Good Documentation Practice

SOP-05 Change Management

SOP-06 Deviation and Nonconformance Management

SOP-07 CAPA Management

SOP-09 Quality Risk Management

SOP-10 Training Management

# Appendices

n/a

# Document revision history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Valid from** | **Description of the revision** | **Reason for the revision** |
| 1 | See header | Document created | QMS implementation |