Guidance for Industry: Computerised System Validation

Version 1.1

Pharmacy and Poisons Board

Contents

1. Introduction

The purpose of this guideline is to provide guidance to industry for risk-based compliance and life-cycle management of computerised systems as required by the *PIC/S Guide to Good Manufacturing Practice for Medicinal Products PE 009-10 - Annex 11 (Computerised Systems)*.

There may be other acceptable approaches that provide an equivalent level of quality assurance. This guideline is not intended to create additional requirements and is not intended to form the basis for GMP inspections.

2. Purpose of this document

To provide guidance to industry on risk-based compliance and life-cycle management of computerised systems.

3. Scope

3.1 In Scope

This guideline applies to all computerised systems used as a part of GMP regulated activities (as covered in PIC/S, Part I and II) including IT infrastructure that supports GMP regulated systems. It outlines the scope and compliance requirements and provides a general approach for the validation of computerised systems.

3.2 Out of Scope

Computerised Systems and IT infrastructure that are not related to GMP regulated activities.

4. Definitions

Process Owner The person responsible for the business process.[1]

Raw Data Any work-sheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities and which are necessary for the reconstruction and evaluation of a work project, process or study report, etc. Raw data may be hard/paper copy or electronic but must be known and defined in system procedures.[2]

System Owner The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.[3]

5. Overview of Computerised System Validation

Validation is an essential part of GMP. It is an ongoing set of activities which continues from the initiation of the project until system retirement. Computerised System Validation (CSV) is performed based on activities that occur throughout the entire life cycle.[4] Therefore, validation activities must be planned, specified, built/configured, verified against the specification, and ultimately reported.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. Computerised systems used in the manufacture of pharmaceutical products should be properly designed, validated and

[1] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annexes, 1 January 2013, Annex 11, Glossary

[2] PI 011-3 PIC/S Guidance Good Practices for Computerised Systems in Regulated “GXP” Environments, 25 September 2007, Glossary

[3] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annexes, 1 January 2013, Annex 11, Glossary

[4] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Glossary

maintained to ensure that the system serves its intended purpose and meets its quality attributes in a consistent manner.

The applications should be validated and it is expected that the infrastructure on which the validated applications are dependent, is compliant and controlled. Therefore, the IT infrastructure which supports the GMP regulated activities should be qualified.

5.1 Risk-Based Approach to Computerised System Validation

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. Several risk assessments may need to be performed at various stages of a computerised system"s life cycle. The objective of quality risk management is to identify, analyse and categorise GMP risks and determine the appropriate controls required to manage these risks.

The risk-based approach will be further discussed in Section 7 "Planning Phase".

5.2 Roles and Responsibilities

In accordance with PIC/S Guide to Good Manufacturing Practice for Medicinal Products PE 009-10 - Annex 11 (Computerised Systems), roles and responsibilities (e.g. Business Process Owner, System Owner, Supplier, IT, etc.) must be clearly defined and documented for the life cycle of a computerised system.

The Process Owner is responsible for ensuring the compliance of the computerised system and has the end-to-end responsibility of the business processes, whereas the System Owner is responsible for ensuring the system is supported, maintained and is available for use throughout the lifecycle. In some instances, the Process Owner may take over the role of the System Owner and vice versa.

Furthermore, responsibilities for writing, approving and authorising documents should also be defined. Activities and responsibilities can be assigned by using a matrix to list the responsible and deliverables for each task.

5.3 Prospective and Legacy Systems Validation

It is expected for validation to be conducted prospectively for all new systems and where possible, for existing systems (legacy systems). However, in the event where legacy systems validation is required, it may be supported by a comprehensive review of historical data in addition to re-defining, documenting, re-qualifying, prospectively validating applications and introducing GMP related life-cycle controls to assure that existing systems are operating correctly.

Good historical data may be used instead of testing. Lack of adequate evidence to support the validation process will make it difficult to perform a meaningful validation and thus can lead to suspension or shut-down of systems if imposing life-cycle controls and testing also cannot be performed.

Retrospective validation is not equivalent to prospective validation and it is not a preferred method for computerised systems; it is used in exceptional cases (continued use is necessary, good data are available and re-testing is not feasible) only and it is not an option for new systems.

5.4 Personnel & Training

Persons involved with computerised systems validation activities should be appropriately qualified in order to carry out their assigned duties.[5]

Personnel and contractors who are responsible for the development, operation, maintenance and administration of the computerised systems must have relevant training, education and experience for the particular system and role.

[5] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 2

Training measures and qualifications should be documented and stored as part of the Quality Management System (QMS).

5.5 ERES (Electronic Records; Electronic Signatures)

Electronic records and electronic signatures are regarded as equivalent to paper records and hand-written signatures. [6] Systems that generate, store or process electronic records or use electronic signatures must be validated.

Electronic records

It must be possible for electronic records to be printed in a readable format.

For batch release related records, it should be possible to generate and print out the changes made to the original data.

Electronic signatures

Electronic signatures should be unique to one individual and there must be procedures to ensure that the owners of the electronic signatures are aware of their responsibilities for their actions, i.e. Users must be aware that electronic signatures have the same impact as hand-written signatures.

Electronic signatures must be permanently linked to their respective electronic records to ensure that the signatures cannot be edited, duplicated or removed in anyway.[6]

Electronic signatures must clearly indicate:

- The displayed/printed name of the signer;
- The date and time when the signature was executed; and
- The reason for signing (such as review, approval, responsibility, or authorship) associated with the signature.

5.6 Documentation Standards and Good Documentation Practices

In a GMP environment, documentation needs to meet certain requirements to ensure product quality and product safety. Therefore, Documentation Standards and Good Documentation Practices are expected to be enforced in the computerised systems validation activities. The following is expected:

- Documents are prepared, reviewed, distributed and stored with care;
- Formal documentation standards are in place to ensure traceability;
- Documents are approved, signed and dated by the appropriate responsible persons;
- Changes to documentation are controlled by versioning and a record of modifications is present;
- Only approved copies of the master protocol, or appropriately identified record books should be used for recording written data;
- All entries are recorded in a clear, legible and indelible way with the minimum possible delay after the event by personnel who witnessed the event;
- Writing errors is corrected with a single strike-out line, initialled, dated and reason explained.

6. The Computerised System Life Cycle

A systematic approach to computerised system validation, which begins with initial risk assessment and continues throughout the life of the system, must be defined to ensure quality is built into the computerised systems.

[6] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 2

Figure 1 shows a suggested general V-model approach for achieving computerised system compliance.

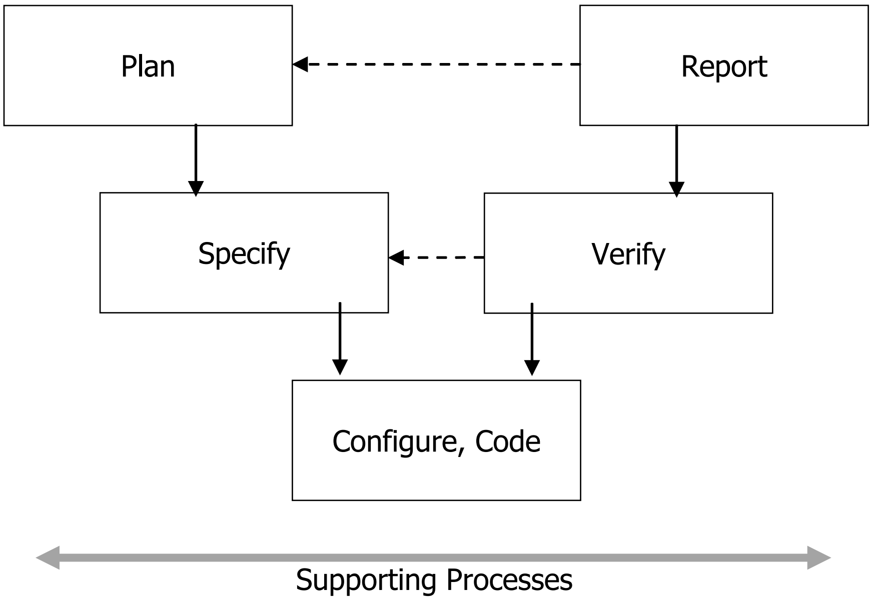

Figure 1 – General V-Model Approach for Computerised System Validation

As shown in the above figure, the specification activities have corresponding verification steps to determine whether the specifications have been met. The required levels of specification and verification may vary depending on the size, complexity and risk of the system.

Risk management is applied throughout the lifecycle to identify risks and to remove or mitigate them to an acceptable level.

An appropriate change control system should be established and applied to both the project and operational phases.

A typical approach to validation based on system complexity and risk is given as a summary below. The GAMP Guide may be referred to, as appropriate, for more detailed guidance.

Category	Description	Typical Examples	Typical Approach
Infrastructure Software	• Layered software (i.e., upon which applications are built) • Software used to manage the operating environment	• Operating Systems • Database Engines • Statistical packages • Spreadsheets (the program itself) • Scheduling tools • Version control tools	• Record version number, verify correct installation by following approved installation procedures • See the *GAMP Good Practice Guide: IT Infrastructure Control and Compliance*
Non-Configured	Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process	• Commercial Off-the-Shelf (COTS) software • Instruments (See the *GAMP Good Practice Guide: Validation of Laboratory Computerized Systems* for further guidance)	• Abbreviated life cycle approach • URS • Risk-based approach to supplier assessment • Record version number, verify correct installation • Risk-based tests against requirements as dictated by use (for simple systems regular calibration may substitute for testing) • Procedures in place for maintaining compliance and fitness for intended use
Configured	Software, often very complex, that can be configured by the user to meet the specific needs of the user"s business process. Software code is not altered	• LIMS • ERP • MRPII • Building Management Systems • Spreadsheets (standard functions) Note: specific examples of the above system types may contain substantial custom elements	• Life cycle approach • Risk-based approach to supplier assessment • Demonstrate supplier has adequate QMS • Some life cycle documentation retained only by supplier (e.g., Design Specifications) • Record version number, verify correct installation • Risk-based testing to demonstrate application works as designed within the business process • Procedures in place for maintaining compliance and fitness for intended use • Procedures in place for managing data
Custom	Software custom designed and coded to suit the business process	Varies, but includes: • Internally and externally developed IT applications • Internally and externally developed process control applications • Custom firmware • Spreadsheets (macros and code)	Same as for configurable, plus: • More rigorous supplier assessment, with possible supplier audit • Possession of full life cycle documentation (Functional Specifications, Design Specifications, structural testing, etc.) • Design and source code review

Figure 2 – General Approach to Computerised System Validation Based on Complexity and Risk [7]

[7] Table M4.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE 2008.

7. Planning Phase

7.1 Risk Assessment

An initial risk assessment should be conducted early in the validation planning process and should identify risks that the computerised system adds to the business process. The initial risk assessment answers the question – do you need to validate, and the results of an initial risk assessment will determine the overall impact of the system. Initial risk assessments must focus on both business and regulatory risks. Further assessments may be required, depending on the outcome of the initial risk assessment.

A lower level risk assessment (Functional Risk Assessment) is used to scale the level of documentation. The higher the rating, the greater the impact on the business and so a greater effort must be made to ensure the system operates as intended. Complex and custom made software has a greater chance of undetected defects compared to Commercial Off-the-Shelf (COTS) software that has been proven to work in the broader market place. For high-risk systems, a full suite of validation documents are required and where the risk is low, a subset is permitted.

Functional Risk Assessments are performed to identify and manage risks to patient safety, product quality and data integrity. The Functional Risk Assessment identifies where you should focus your efforts in terms of documentation and testing. Areas identified with a high risk priority should be the focus for closer attention and should be „designed out" as much as possible.

Note that in order to appropriately manage risk and to maximize leverage with a potential supplier, supplier evaluation must be done during the selection process, not after the supplier has been selected.

7.2 Validation Plan (VP)

The purpose of a VP is to define the activities, procedures, and responsibilities for establishing the adequacy of the computerised system. The plan must be approved prior to commencing formal validation activities, and serves to guide all subsequent validation activities.

The plan defines:

- what activities are required;
- how they will be performed and who will be responsible;
- what their output will be; and
- how compliance will be maintained for the lifetime of the system.

The plan should document the intended use of the computerised system and must take into account the regulatory impact (e.g. GMP) of the system. The business impact should also be considered. The system novelty, complexity and results from supplier assessments should be considered when determining the validation planning process.

The VP should also outline the processes and services that will be used to support the project (e.g. Documentation Management, Deviations Management, Configuration Management, Change Control management and Data archiving).

Training of project team members on these supporting services should be determined and documented either in the VP or elsewhere in the QMS.

The table of contents of a typical VP is given below:

- Introduction and Scope / Scope Inclusions and Exclusions
- System Description / Overview
- Roles and Responsibilities / Organisational Structure
- Assumptions, Exclusions and Limitations
- Risk Assessment

- Validation Strategy / Approach
- Deliverables
- Acceptance Criteria
- Change Control
- Document Control
- Configuration Management
- Test Deviation Management
- Standard Operating Procedures and Training
- Supporting Processes
- Reporting and System Release
- Glossary
- Revision History

7.3 User Requirements Specification (URS)

The URS is a critical document that defines, clearly and precisely, the requirements of the computerised system and agreement to the requirements from all affected by the system implementation. The URS should be the definitive statement of what the system must or must not do and be traceable throughout the lifecycle.

The URS should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact[8].

The URS should be:

- Complete - Functionality missed in the URS will be at risk of not being tested;
- Realistic - Specified functions that cannot be implemented will delay the project;
- Definitive – The requirement must be clear and unambiguous. There should be no conflict between requirements;
- Testable - Functions that are not testable cannot be validated.

The URS must also define non-software requirements (e.g. SOPs) and hardware. SOPs must be considered for both the day-to-day use of the system by the end users and also system administration by the support personnel. Non-functional requirements such as maintainability and usability can also be included. There should be a clear distinction between mandatory regulatory requirements and optional features.

The URS should be understood and agreed by both the user and supplier. This is important for the software supplier to accurately translate user needs into useful functionality. Once agreed, the software engineers can then commence the preliminary design to establish exactly what functions are required for each of the items specified in the URS.

It is common for computerised systems to evolve through modification and enhancements due to additional business or regulatory requirements, when this occurs, the URS must be updated.

7.4 Supplier Assessment

The supplier assessment is an important input to the validation planning process. This assessment is intended to ensure that system/service suppliers are selected based on their capability to provide quality systems/services and documentation which is adequate for validation[9]. The regulated company therefore should have in place procedures and records that indicated how and on what basis suppliers were selected.

The decision whether to perform a supplier assessment and the scale of assessment should be documented and based on a risk assessment and categorization of the system components. The assessment can be a questionnaire, third party audit or a direct on-site audit.

[8] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 4.4

[9] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 3.4, 4.5

The regulated user should take all reasonable steps to ensure that the system has been developed in accordance with an appropriate quality management system. Compliance with a recognised QMS may provide the regulated user (and regulatory agencies) with confidence in the structural integrity and operational reliability of the software product. Structural integrity and the application of good software and hardware engineering practices are important for critical systems. Quality cannot be inspected or tested into software. Poorly written software can expose the regulated company to ongoing risks.

If supplier documentation or work is leveraged to simplify validation efforts, the degree to which reliance is placed on supplier documentation must be based on the outcome of the supplier assessment. Note that assessment information relating to suppliers or developers of systems and services should be made available to inspectors on request.

8. Specifications Phase

8.1 Functional Specifications (FS) and Design Specifications (DS)

The FS provides a written definition of what the system does and what functions are provided. The DS is the detailed description of the equipment design that contains information on how the system is to be built and maintained. These specifications are normally written by the developer and should define a system to meet the URS, i.e. the customer's needs. Each entry in the URS should be addressed in the FS and DS.

FS and DS should be prepared for bespoke equipment and be reviewed by the customer. For small systems, the URS and FS may be included in the same document. The specifications must be reviewed to verify traceability from the URS through to design.

8.2 Configuration Specifications

Configuration Specifications document the „as built configuration“ and design of software systems, servers, network, desktops or printers where appropriate.

Configuration Specifications are an important part in maintaining the integrity of the software system/service during its life cycle.

9. Implementation & Verification Phase

For purchased customised systems or internally developed systems, the owner must ensure suitable control around the construction and coding. For configurable systems, a configuration baseline must be established in order to define the system at the start of validation testing.

Naming conventions and programming practices should be defined. A Source Code review may need to be carried out and the rigor of the Source Code review and documentation should be scaled to the risk profile of the computerised system.

9.1 Verification activities

Testing must demonstrate that all requirements, specifications and design have been met.

The extent of testing shall depend on a documented risk assessment that evaluates the following criteria:

- Impact on product quality
- Impact on business continuity
- Complexity of system
- Information from the vendor on type of tests and test environment
- Level of customization

Test Strategy

A testing strategy should detail the planned test phases, roles and responsibilities for creating, approving and execution test protocols, documentation of deviations and anomalies. The testing strategy may be documented in the VP. Any testing that will be carried out by the supplier must also be noted in the testing strategy.

Automated testing tools and test environments should have documented assessments for their adequacy. Deviations, including unexpected results and test failures, must be logged. Management of deviations should be detailed as part of the testing strategy.

Test scripts should be developed, formally documented with test methods and used to demonstrate that the system has been installed, and is operating and performing satisfactorily. These test scripts should be related to the URS and the FS defined in the Planning and Specification Phases.

Installation Verification

Installation Verification (or Installation Qualification) verifies that the required physical hardware and software components have been installed and configured correctly in accordance with the platform and DS. Test specifications should specify how certification results and other tests and verifications together satisfy the required level of IQ. Testing activities include:

- Verification of documentation;
- Verification of correct environmental conditions;
- Installation of servers and clients;
- Installation of network devices; and
- Record configuration settings.

Functional Testing

Functional Testing (or Operational Qualification) verifies that the system operates in an expected manner as defined in the respective specifications. Testing activities include:

- Interface and I/O testing;
- Testing of functionality defined in specifications;
- Testing of system process parameters limits, alarms and interlocks;
- Error handling;
- Backup and recovery; and
- Security and access control.

User Acceptance Testing (or Performance Qualification) must demonstrate that the system consistently performs and involves testing the system with the entire application or business process. Tests must be traceable to the URS and must verify that the key functions of the system work as intended. System operation and support SOPs must also be verified.

9.2 Data Migration

There might be the need for data migration as part of the project activities. This is the case when:

- transfer of data to another format/system/platform; and
- converting data as part of a system upgrade.

Data migration must include tests to assure acceptable accuracy and completeness of data migration. Data should not be altered in value and/or meaning during migration process.[10] A final report is recommended to summarize the status. Additional Functional Testing could also be required and will be specified in the VP.

9.3 Traceability

[10] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 4.8

A traceability matrix should be created to document traceability between requirements, design documentation (where applicable) and verification activities. [11] The scope of the traceability varies based on the system complexity.

9.4 Acceptance Criteria

Acceptance of the system as being fit for release for operational use is only after demonstrating satisfactory completion of all testing and verification activities. Acceptance criteria can be documented in the VP. Once the acceptance criteria are fulfilled, the system can be reported and handed-over.

10. Reporting & Handover (System Release) Phase

The transfer from project stage to operational stage must be well managed. After all validation activities are completed, a Validation Report (VR) must be written and approved in order to define the controlled transfer of the computerised system to the production environment. Quality Assurance department and the Process Owner should be included on the approval list.

The VR should provide:

- a brief, single point of reference for qualification results and an assessment of the completion status of the qualification and validation work, essentially reporting on all aspects discussed in the VP;
- any unplanned change from the VP or any failure to meet any acceptance criteria;
- all related incidents that have been closed or otherwise justified as acceptable;
- training programs are completed and documented for all related personnel involved with the system; and
- that the system has been reviewed and assessed as fit for its intended purpose.

It is expected for the QMS to be based on a lifecycle concept providing evidence that a specified standard of quality has been met and is continuously improving. A compliant status of the system will be maintained through the QMS which must include formal procedures covering all aspects of the operation phase.

Preparation of SOPs is a part of the hand-over activities and must be completed before system go-live.

11. Operations Management

Once a computerised system has been validated and released for use, it is important to maintain its compliant state throughout its operational life. This can be accomplished by:

- the implementation of an adequate maintenance system;
- a documented process for tracking and monitoring the systems performance; and
- training.

The following issues need to be covered as applicable in procedures:

11.1 Operation of the system

A high-level overview of the computerised system can be provided, this may include system diagrams, process flows and system functions. Detailed work instructions describing the use and maintenance of the system can also be provided.

Main tasks and responsibilities of the users engaged in the operational activities should be defined. The suppliers may be involved in the support and maintenance activities.

11.2 Data Integrity

[11] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 4.4

For electronic records, regulated companies should define what data is to be used as raw data. At least all data on which quality decisions are based should be defined as raw data.

Adequate checks for the accuracy and consistency if data must be implemented to ensure that data integrity is maintained throughout the life cycle of the computerised system.

Accuracy checks need to be performed independently by another individual or through validated electronic systems for critical data entered manually to prevent incorrect data entry. [12] The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

Access must be restricted to authorised persons and appropriate access control checks should be conducted regularly. It is expected that appropriate controls will exist such as the maintenance of a register of authorised users, identification codes, scope of authorised actions, in support of GMP electronic records and electronic signatures.

Periodic checks must be in place to ensure the data backup is taken regularly and is restored in an accurate and consistent manner. Inputs/Outputs (I/Os) should be monitored to prevent inaccurate data inputs and outputs and to ensure the process remains within the established parameters. For any anomalies, the cause should be investigated, corrective action should be taken and revalidation should be considered.

11.3 Change and Configuration Management

Configuration Management provides a basis for ensuring an orderly control of configuration elements produced by IT and an effective mechanism for incorporating software changes, both during development and operations.

All changes made to the computerised systems must be managed with a formal procedure, due to the impact they may have on the validated system.[13]

The changes shall include modifications made to the configurations of systems, as it is important for configuration of systems to be managed so that the system can be restored to its intended configuration if necessary.

Changes should be formally requested, documented and approved before implementation. The change records must describe the actions to be taken, the evaluation of the proposed change (i.e. to assess impact and risk of implementing the change), including the need and extent of qualification and validation activities to be performed.

A configuration plan may be used to:

- describe naming convention and nomenclature for version numbering of system components and documents;
- list all software components and documents with respective version numbers and periods of use; and
- describe the procedure and tools required to update software versions.

11.4 Periodic Review

Computerised systems should be periodically reviewed in order to ensure the systems remain in a validated state.

The results of the assessment should be formalised in a periodic review report stating, where applicable, all changes to system, deviations, incident and problems, security issues and overall validation status.[14]

Based on the periodic review assessment results, revalidation may be required due to major changes outside the control of a regulated company that could have an effect on the process or

[12] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 6

[13] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 10

[14] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 11

product quality or due to the system being out of control. The extent of revalidation will depend on the significance of changes and it should be subject to change control. The need for revalidation should be the absolute last resort and should be avoided by change management, configuration management, periodic review and evaluation.

11.5 Incident and Problem Management

An incident management approach must be defined to ensure that any unplanned issues that could impact patient safety, product quality and data integrity are addressed before any harm occurs.

A problem management system should exist that defines the activities required to identify the root cause of incidents and their solutions by using appropriate change control procedures.

If an incident or a problem triggers a change to a validated system, the incident/problem records and change control records must be cross referenced.

Incident reports must be monitored over time to assess if incidents are indicative of a broader problem. They should also be included in the validation periodic review activities along with the problem logs.

11.6 Security Management

Physical and logical security controls must be applied to computerised systems in order to prevent unauthorised use and to ensure that data is adequately and securely protected against intentional or accidental loss, unauthorised change, damage or removal.

The controls may include use of key locks, pass cards, biometric controls and username-password combinations.

Security roles and responsibilities must be clearly defined and changes made to authorisations should be recorded.

In the event when the computerised system is used for batch release, the system should only allow authorised persons to certify the release of batches. There should be a clear identity of the person releasing the batch.[15]

11.7 Audit Trails

An audit trail is a log generated by the computerised system that allows operator entries and actions that create, modify, or delete GMP relevant electronic records to be traced back to the original electronic record. A decision on whether to implement an audit trail must be based on a documented risk assessment.

An audit trail is expected to have the following features:

- access to audit trail data should be limited to print and/or read only;
- it must be protected against modification or deletion;
- it should have the ability to capture a full history of all GMP related transactions, including the identity of the person making the change, the date and time of change and the reason for change;
- the date and time of the audit trail must be synchronised with a trusted date and time service e.g. main server;
- it should be readily available in a readable format.

Audit trail configurations and logs must be reviewed regularly based on the criticality of the system. Audit trails may be requested by GMP inspectors as evidence.

11.8 Backup and Recovery

[15] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 15

There should be formal procedures in place to ensure that routine back-ups of all GMP related data (including audit trails) are made and stored in a secure location at a frequency based on a risk analysis to prevent intentional or accidental damage.

There must also be periodic checks in place to ensure backups are recoverable and data integrity and accuracy is maintained during the recovery process.

11.9 Disaster Recovery and Business Continuity

A disaster recovery procedure should be available that defines the management of operations in the event of a breakdown, in order to establish the continuity of business processes.

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

Disaster recovery plans and procedures must be documented and tested periodically.[16]

12. System Retirement

When a computerized system requires retiring, a retirement plan must be developed to ensure that regulatory or business critical data is appropriately transitioned without loss of information. It is the Process Owners responsibility to manage the replacement or withdrawal of a software system from use.

12.1 Data Archiving/Disposal

Although the software has reached the end of the life cycle, there may be a requirement to retain certain regulatory or business critical data for a predefined retention period. Therefore the data must be either archived or migrated to another system.[17]

Procedures must be in place and periodic checks must be performed to assure that data integrity and accuracy is maintained and recoverable throughout the required retention period. Access to data should be ensured throughout the retention period.

Once the archived data reaches the end of the retention period, the data may be destroyed or the retention period may be extended.

12.2 Data Migration

There might be the need for data migration as part of the project activities. This is the case when:

- Replacing software or an application; and
- Converting data as part of a system upgrade.

Data migration must include tests to assure acceptable accuracy and completeness of data migration. A final report is recommended to summarize the status. Additional Functional Testing could also be required and will be specified in the VP.

12.3 Decommissioning

Formal decommissioning of the computerised system typically occurs when the system is retired from use. However, in some circumstances, a computerised system may remain in a read-only state for a period of time to permit data access. In this case, decommissioning will occur when the requirement to access the data has expired.

[16] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 16

[17] PIC/S Guide to GMP for Medicinal Products (PE 009-10) – Annex 11, Clause 17

Document Information

Version	Date	Description of Change
1.0	27 Dec 2013	First version
1.1	Sept 2024	Reformatting of version 1.0

References

Document Title
PIC/S Guide to Good Manufacturing Practice for Medicinal Products PE 009-10 (Part I and II)
PIC/S Guide to Good Manufacturing Practice for Medicinal Products PE 009-10 - Annex 11 (Computerised Systems)
GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems

DOCUMENT END