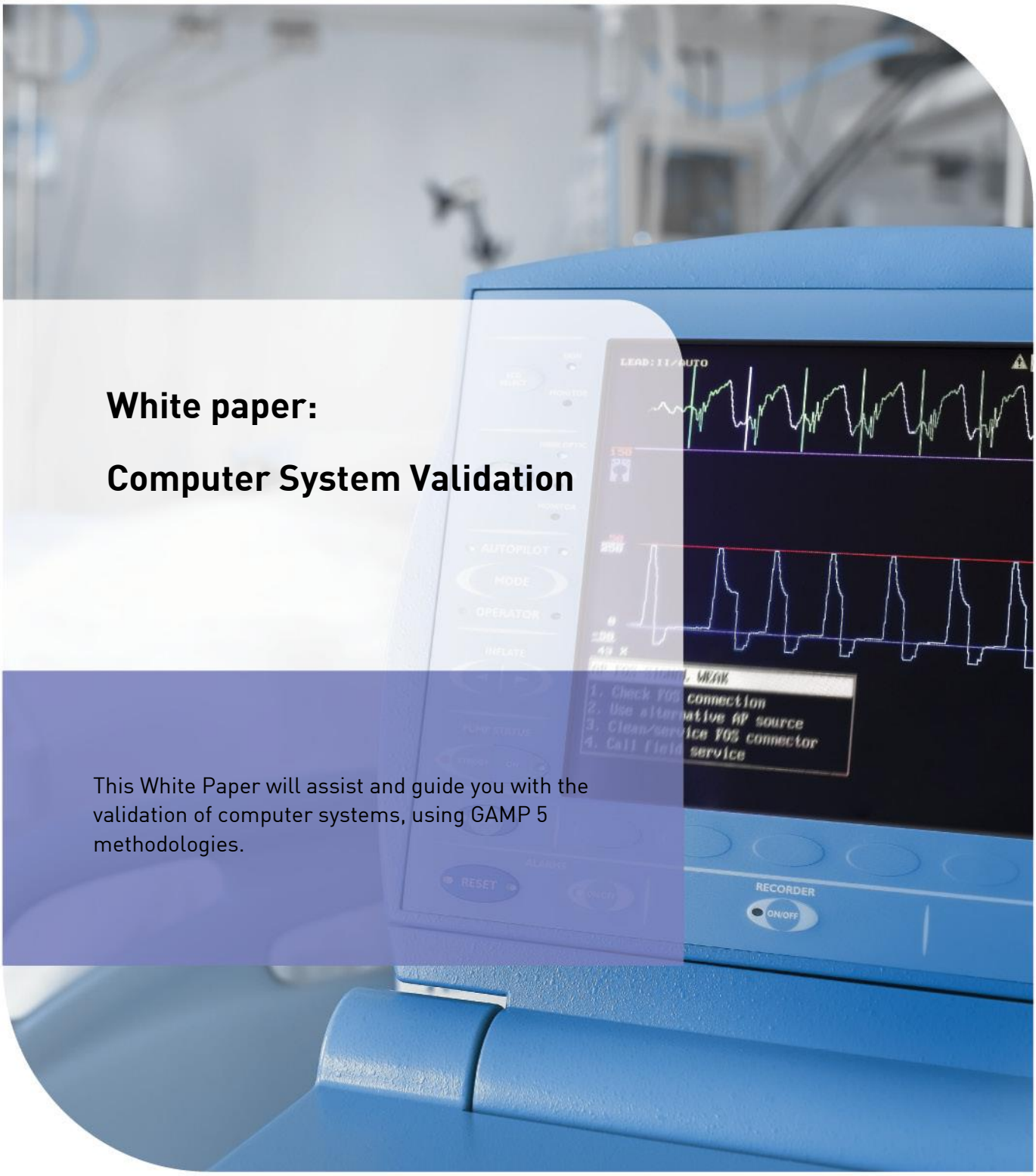

White paper:

Computer System Validation

This White Paper will assist and guide you with the validation of computer systems, using GAMP 5 methodologies.

PharmOut®

MKT_TMP200_01_r06

Introduction

This whitepaper is intended as a guide to assist your organization with Computer System Validation (CSV) and provides an overview of CSV methodologies and a road map of deliverables used in the CSV process. As computer systems are diverse, depending on the type and size of system, novelty, complexity and business impact, the deliverables may be scaled up or down accordingly.

The CSV process discussed in this whitepaper is based on the GAMP 5 framework, as it provides an excellent and pragmatic approach for CSV which, when followed, will ensure your computerized systems are fit for purpose, will meet the needs of your business, and are compliant with current regulations.

Validation Process

The range of activities required to validate a computerized system are determined by its GAMP 5 software and hardware categorization, GxP impact, applicable electronic records and electronic signatures requirements,and its risk-based lifecycle approach.

There are four life cycle phases of a computer system which are employed by GAMP 5 - concept, project, operation and retirement. Various activities take place in more than one phase, hence a fifth phase, multi-phase, is documented here to describe these cross phase activities.

Concept Phase

System Software and Hardware Categorization

The following GAMP 5 software and hardware categories are used to establish the validation approach and determine the deliverables:

- Category 1 – Infrastructure Software
- Category 3 – Non-Configured Products
- Category 4 – Configured Products
- Category 5 – Custom Applications
- Hardware Category 1 – Standard Hardware Components
- Hardware Category 2 – Custom Built Hardware Components

GxP Impact Assessment

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 Records and Electronic Signatures (ERES) Assessment

An assessment is carried out to establish if the system needs to meet the requirements of electronic records and electronic signatures by determining what electronic records are created by the system, how those records are maintained and how the records will be signed, either by hand or electronically.

Project Phase

Supplier Assessment

The system supplier must be assessed to determine their suitability to provide a quality system that meets all requirements. Confidence will be gained through their adherence to a documented Quality Management System and Software Development Life Cycle (SDLC).

The assessment may take the form of a basic checklist, a postal questionnaire, or an onsite audit, depending on the outcome of the risk assessment. Supplier selection should then be documented in a report, along with whether the supplier documentation will be leveraged or not.

Risk Management

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.

Validation Plan (VP)

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.

System Overview

The system overview is a brief description of the system and includes:

- System identification
- Business processes the system supports
- Data managed by the system
- High level functionality of the system
- High level schematic diagram of system architecture/hardware
- All interfaces to external systems
- How data is secured by physical or electronic means

The system overview may be incorporated into a section of the VP.

User Requirements Specification (URS)

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 and testing

Functional Specification (FS)

The Functional Specification (FS) defines the full system functionality including how the user and business requirements are satisfied. It is the basis for system design, customization, development and testing. Supplier documentation should be leveraged wherever possible or referenced from the FS. It must be clear how the requirements are met from the URS and provide sufficient information to allow the design specification to be written.

The FS may be combined with the URS as a Functional Requirement Specification (FRS).

Configuration Specification (CS)

The Configuration Specification details the configuration parameters and how these settings address the requirements in the URS. This may be a standalone document or detailed in the FS.

Design Specification (DS)

This activity involves documenting both the hardware and software as a combined document (DS) or for larger systems as two separate specifications, Hardware Design Specification (HDS) and Software Design Specification (SDS).

It can be merged with the Functional Specification as the Functional Design Specification (FDS).

Design Review (DR)

Design Reviews are conducted to verify that the design conforms to required standards; the FS meets the requirements defined in the URS and that the requirements can be traced through the design documents in preparation for testing. The output from the risk assessment is also considered in the review process.

A design review report documents the outcome of the design review process.

Software Development

This is a process where source code is planned and written in accordance with pre-defined programming standards.

Code Review

If applicable, a code review is performed to detect and fix coding errors before the system goes into formal testing. It verifies that the software has been developed in accordance with the design and programming standards have been followed.

Data Migration

A Data Migration Plan is created when a system requires data loading from an existing system. It describes the activities and deliverables required to select, remove, cleanse, migrate and verify all data to assure its security and integrity. Data can be manually or automatically loaded/migrated, however if any critical data has been manually entered, an evaluation should be carried out to ensure its correctness.

Testing

Testing is carried out to verify that installation and configuration has been conducted in line with specifications and that the functionality is challenged at subsystem and system level. This verifies that system components perform their tasks separately, that the subsystems integrate correctly and that the system meets the requirements and expectations of its users.

The testing approach is described in a test plan as either a section within the validation plan or as a standalone document. Where possible at each stage, any previous testing should be leveraged, which is defined in the plan. The plan also defines the different types and details the level of testing (e.g. installation, unit, system, acceptance) that will be required for a project. The results from the outcome of the risk assessment will define how precise the depth and rigor of testing shall be and the level of testing will be scaled appropriately. The plan will specify the test environment (development, test, or production) in which testing shall be performed, the use of any tools to be employed for testing and test data requirements.

The installation verification, functional verification and requirements verification testing documents are generated against pre-approved specifications. Test cases are written in test steps as instructions to be followed to test whether the system satisfies the defined acceptance criteria appropriate for the test level. The test steps are written in sufficient detail so that testing is repeatable with consistent results. A printed copy of the approved test case document is executed and the test steps annotated to record the test results. Verification against the expected result defines whether the test step is a pass or fail. Evidence produced during test execution (e.g. reports or screen prints) is attached to allow an independent review and approval of the results. Test results are reviewed, summarized and approved as a standalone test report or as part of the executed document.

System Operating Procedures / User Manuals

System Operating Procedures should be written to provide clear unambiguous instructions to personnel as to the accepted process of completing a particular operation in a systematic, consistent and safe manner. User manuals should be leveraged wherever possible.

Training

Key users must be trained in the use of the system software, applications and procedures as necessary for the development, maintenance, testing and support of the system.

System Support Plan

A System Support Plan defines the supporting organizations and procedures to support and maintain the quality/validation of the system during its operation phase.

Service Level Agreement (SLA)

A Service Level Agreement (SLA) documents a mutual agreement for the service provided between all parties. It should clearly define service, document and data ownership and ensure accountability, roles and responsibilities are established. The escalation process should be fully described along with the service performance criteria.

Handover

A plan should be written to define when the application will transition into the operation phase and how any disruption will be managed. The risk management process could be used in this process together with a back out plan. It should ensure that project and validation / verification deliverables are complete prior to handover.

System Release

When the system is ready to be released for routine use, a certification statement is created detailing the following:

- System name and version
- Date of release
- Department using the system
- The activities and deliverables relating to the release
- Restrictions on use (if any)
- Open incidents (if any)

Deployment Planning

Deployment activities include the installation, configuration, data migration and testing of the system and components on the final operating environment (production).

Validation Report (VR)

The Validation Report (VR) summarizes the activities carried out during the project, describes any deviations, with justification, from the Validation Plan (VP), lists any limitations or restrictions on use, summarizes any incidents and details any outstanding and corrective actions.

A certification statement concludes whether the validation was successful or not and approves or declines the system for its intended routine use.

An Interim Validation Report may be issued if all post go-live activities are not complete.

Operation Phase

The computer system is now in operation. In order for it to maintain its validated status, all aspects of the system and operating environment must be kept in a documented state of control. The following activities will assist in this phase.

Backup and Restore

Backup and restore is a routine process consisting of copying software, data and electronic records to a separate safe and secure area. This information is protected, available and when required, able to be restored, uncorrupted in its original format.

Backup and restore is not the same as the archiving and retrieval processes.

Continuity Planning and Testing / Disaster Recovery

The continuity plan defines the approach to test all or part of a system's restoration process. This verifies the activities required to get a system or its component parts in an operating condition again in the event of a disaster.

Periodic continuity testing should be conducted as a tabletop or full test to verify recovery processes are up to date. A schedule is created to detail the test type and frequency depending on system criticality and risk.

Periodic Review

The cumulative effect of changes to a system could affect its validated status. Periodic reviews are performed to ensure that the computer system remains within both company and regulatory compliance, and is fit for its intended use. The review evaluates the compliance status of the entire system and plans any required corrective action activities.

The frequency of review depends on such things as system criticality, risk, business impact and complexity; however the frequency interval is generally not greater than 3 years.

Data Archive & Retrieval

Data archiving is the process of removing data and electronic records that is no longer actively used to a separate, secure data storage area for long-term retention. Data that must be retained for regulatory compliance has to be archived and be available for retrieval when required.

Records retention requirements should also be considered with respect to the protection, preservation, and confidentiality of electronic records, including their associated audit trail information.

Archiving and retrieval is not the same as the backup and restore processes.

Retirement Phase

Decommissioning

A decommissioning plan must be prepared for systems that are to be retired from operational service so that the process is documented and controlled.

Consideration must be taken into account with regards to the archiving of data and records retention requirements, along with any hardware disposal.

Multi-Phase

Requirements Traceability

Traceability must be documented to identify the connection between the results of the risk assessment, via the requirements specification, design and through all testing to individual test cases.

Change Management

The change management process defines the requirements for assessing, documenting and managing changes to ensure systems remain in a validated state and applies to software, hardware, configuration data and documentation.

The process requires all planned and unplanned changes to be planned, assessed, executed and closed in a controlled and compliant manner.

Project change control is used to manage changes made to any approved primary design documents, project scope changes or changes that will have an effect on product quality, patient safety, data integrity, project cost or schedule.

Incident / Deviation Management

The incident / deviation management process defines the requirements for managing incidents / deviations for the entire system lifecycle. It details the recording, analyzing, resolution and closure of faults, anomalies and problems that have been identified during the project phase, testing and operation of the system.

Incident logs should be created to allow the collection and tracking of incidents.

Document Management

The document management process defines the lifecycle controls for documentation including the creation, review, approval, storage, archiving and distribution of documents. It describes how documents are classified, named, numbered and maintained, and also the mechanism for updating them.

It is applicable to both hard copy (paper) and soft copy (electronic) documents.

Configuration Management

The configuration management process defines the identification, control and status for configuration items (e.g. software, objects) which are under change and version control; as well as the controls, procedures, tools and processes to manage the configuration modifications.

Access and Security Management

The access and security management process defines the requirements for the security and integrity of a system. Physical and logical security protection mechanisms should secure the system and data against deliberate or accidental loss, damage or unauthorized change.

Access requests and permissions should be defined with regard to the initiation, authorization, amending, revoking, recording and auditing of access rights.

Validation Deliverables Checklist

Deliverable	Required? (Yes / No)	Complete? (x / ✓)
Multi Phase		
Requirements Traceability Matrix		
Change Management		
Access and Security Management		
Document Management		
Incident / Deviation Management		
Configuration Management		
Concept Phase		
GxP Impact Assessment		
System Software and Hardware Categorization		
Electronic Records and Electronic Signatures Assessment		
Project Phase		
Supplier Assessment		

Deliverable	Required? (Yes / No)	Complete? (x / ✓)
Risk Assessment		
Business Requirements / Process Requirements		
System Requirements		
User Requirements Specification		
System Overview		
Validation Plan		
Configuration Specification		
Functional Specification		
Functional Design Specification		
Hardware Design Specification		
Software Design Specification		
Unit Specification		
Design Specification		
Design Review		
Programming Standards		
Code Review		
Data Migration		
Test Plan		
Factory Acceptance Testing Protocol / Report		
Installation Qualification Protocol / Report		
Unit and Integration Testing Protocol / Report		

Deliverable	Required? (Yes / No)	Complete? (x / ✓)
System Test Protocol / Report		
Operational Qualification Protocol / Report		
Acceptance Test Protocol / Report		
Performance Qualification Protocol / Report		
System Operating Procedures / User Manuals		
Training		
System Support Plan		
Service Level Agreement (SLA)		
Handover		
System Release		
Deployment Planning		
Validation Report		
Operation Phase		
Continuity Planning / Testing / Disaster Recovery		
Periodic Review		
Data Archive & Retrieval		
Backup and Restore		
Retirement Phase		
Decommissioning Plan / Report		

References

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

Sources

Links used within this document are prone to change. Please refer to the appropriate source for the most recent information. We endeavour to keep an up-to-date record of information at www.pharmout.net

PharmOut Pty Ltd, ABN: 85 117 673 766, Unit 10, 24 Lakeside Drive, Burwood East, Victoria 3151.
Ph: +61 3 9887 6412, Fax: +61 3 8610 0169, Email: info@pharmout.net Web: www.pharmout.net

PharmOut is an international GMP consultancy serving the Pharmaceutical, Medical Device and Veterinary industries. PharmOut specialises in PIC/S, WHO, United States FDA, European EMA, and Australian TGA GMP consulting, engineering, project management, training, validation, continuous improvement and regulatory services.

Our team includes international GMP experts who have previously held leadership roles within regulatory bodies.

For more information please visit www.pharmout.net or contact us at info@pharmout.net.

PharmOut Pty Ltd, ABN: 85 117 673 766, Unit 10, 24 Lakeside Drive, Burwood East, Victoria 3151.
Ph: +61 3 9887 6412, Fax: +61 3 8610 0169, Email: info@pharmout.net Web: www.pharmout.net