This Guide discusses the considerations which should explain this activity and suggests a process to be followed in order to assess and validate Legacy Systems.

Reprinted from
PHARMACEUTICAL ENGINEERING®
The Official Journal of ISPE
November/December 2003, Vol. 23 No. 6

GAMP Good Practice Guide: The Validation of Legacy Systems

by the ISPE GAMP Forum

1 Introduction

In view of the rapid evolution of both new technologies and regulatory expectations over recent years, it is crucial that pharmaceutical organizations take positive action to maintain their existing cGxP-related systems in a validated state. This Guide discusses the considerations which should explain this activity and suggests a process to be followed in order to assess and validate Legacy Systems.

2 What is a Legacy System?

There is no formally accepted definition of 'Legacy System,' but for the purposes of this GAMP Good Practice Guide (GPG), a Legacy System should be considered to be any GxP relevant system that is in place and in use, and which is deemed not to satisfy current regulatory expectations.

It is **not** acceptable under any circumstance to implement a new system that has not been validated. Legacy System validation "is not equivalent to prospective validation and is not an option for new systems." (Ref: PIC/S PI-011-1.)

3 Typical Issues Encountered with Legacy Systems

There is a risk that a Legacy System, which has not been the subject of a recent validation program, will fail to comply with current regulatory expectations, e.g., 21 CFR Part 11. Therefore, there is a need to review existing systems for compliance. Typically, the issues are associated with:

- ownership of the system
- validation package
- security
- system functionality
- data integrity
- archiving of data

3.1 Ownership of the System

The owner of a Legacy System has the responsibility to ensure that:

- the system continues to be relevant to the (GxP) process being supported
- the operating procedures are up-to-date
- user training is sufficient to maintain the competence of the users
- a formal change control procedure is in place and is followed
- any necessary maintenance agreements, (e.g., Service Level Agreements,) are in place and valid

Essentially, the owner of a Legacy System should ensure that an appropriate validation package exists.

In this age of mergers, acquisitions, divestments, outsourcing, and reengineering of organizations, operational responsibilities are frequently reorganized. As a result, the ownership of existing systems may become poorly defined or unknown. Without a formal and controlled hand-over process, it is unlikely that the knowledge associated with a particular system will be passed to the new owner, or even that the

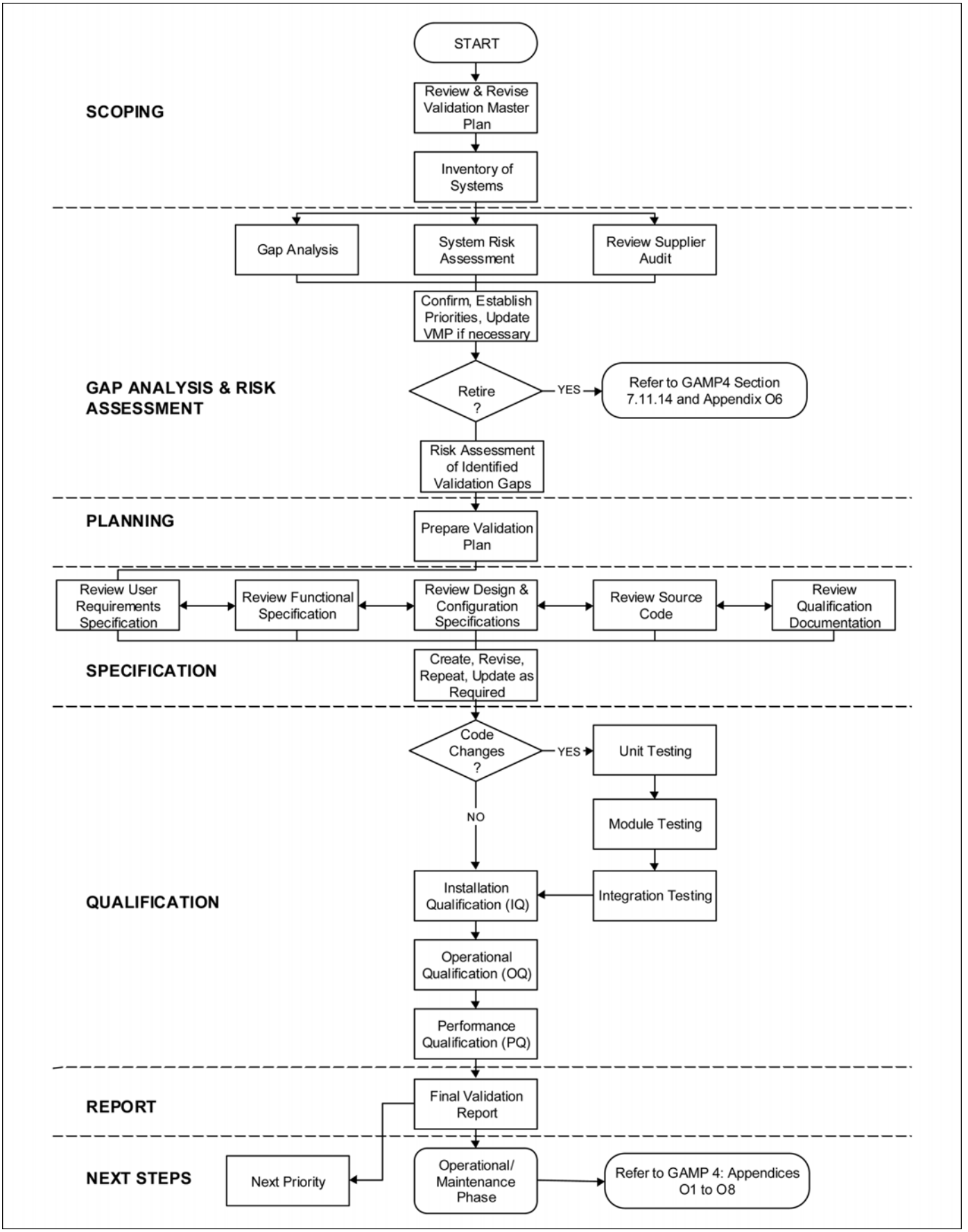

Figure 1. Legacy Systems Validation Activities.

location of critical system documentation will be made known to the owner. An incoming owner must take appropriate steps to identify those systems under his ownership. When a system has no owner, it will fall into an uncontrolled state.

It is, therefore, critical that the system owner be clearly identified, whether an individual or a representative team accountable for widespread or enterprise systems.

3.2 Validation Package

It is usually the case that documentation associated with Legacy Systems is no longer up-to-date or complete. The Legacy System may have been validated to an earlier regulatory expectation that is no longer adequate. With changes in the use of a Legacy System, parts of the system documentation may no longer reflect accurately what the system does, how it does it, or how it should be used. All such issues need to be remedied in a Legacy System validation program, which should produce a validation package for the Legacy System.

The required validation package consists of the system documentation, together with the qualification documentation, fronted by a Validation Plan and concluded by a Validation Summary Report.

3.2.1 System Documentation

In the context of this GPG, system documentation should be regarded as the 'live' documents, such as specifications (e.g., URS, FS, design/configuration specifications, source code), Requirements Traceability Matrix, Standard Operating Procedures (SOPs), user reference manuals, and 'Help' text. Without the application of a formal change control procedure, the 'live' documents will fail to represent the system accurately.

3.2.2 Qualification

Qualification provides the documentary evidence that the system does what it is supposed to do, accurately and consistently. For Legacy Systems, the qualification documentation may not be available or may not be adequate in terms of current regulatory expectations. Existing documentation also may have failed to incorporate the qualification of any changes that have been made to the system since it was first implemented.

3.3 Security

Security is frequently an issue with Legacy Systems; particularly with the advent of ISO17799, there is an increasing focus on the physical and logical security of the system and its data. All systems which contain electronic records and are subject to validation, must be able to demonstrate that access to the system is properly controlled. It also is a requirement that, where appropriate, there are multiple levels of security, e.g., users may have different access rights from supervisors, who should have different access rights from the system administrator. The way in which access rights are granted also may need to be addressed.

Issues relating to security are addressed in the Good Practice and Compliance for Electronic Records and Signatures, Part 2: Complying with 21 CFR Part 11: Electronic Records and Electronic Signatures and in GAMP 4, Appendix O3.

3.4 System Functionality

Changes to regulations or their interpretation may have caused the capabilities of the Legacy System to be regarded as inappropriate or inadequate. For example, the Legacy System might not have the capability to record audit trails that are now required for compliance with 21 CFR Part 11.

With increasing concern about the control of electronic records and signatures, the availability of audit trails has become a prominent issue. The audit trail needs to record who did what, when they did so, and retain the original value for any altered data; again, this is addressed in the Good Practice and Compliance for Electronic Records and Signatures, Part 2: Complying with 21 CFR Part 11: Electronic Records and Electronic Signatures. Many Legacy Systems do not have an audit trail facility although some will provide a transaction history for a limited number of batches and then overwrite that data.

These are issues to be addressed when reviewing the status of Legacy Systems and deciding appropriate actions to remedy those issues in order to bring the Legacy Systems into compliance with current regulatory expectations.

3.5 Data Integrity

Where a Legacy System failed to demonstrate the accurate and consistent capture, change, and retention of data during a prior validation effort, and for systems which have never been validated, it may not be possible to show the integrity of the data now residing within the Legacy System.

3.6 Archiving of Data

Data archived from the Legacy System is often overlooked, but must be retained in a secure and accessible manner. Further guidance is provided in GAMP 4, Appendix O6: *Guideline for Record Retention, Archiving, and Retrieval*.

4 Objectives of Legacy SystemValidation

The objectives of validating a Legacy System are fundamentally the same as for prospective validation except that, being accomplished after the system is 'in place and in use,' some elements of the validation process have already occurred.

Typical objectives of Legacy System validation include:

- to ensure that the Legacy System properly supports the process
- to ensure that the Legacy System has been properly installed, is operated correctly, and that procedures and practices are in place to allow it to be maintained in a state of control throughout its useful life
- to establish a complete set of system documentation providing a precise definition of the operating environment, functionality, hardware and

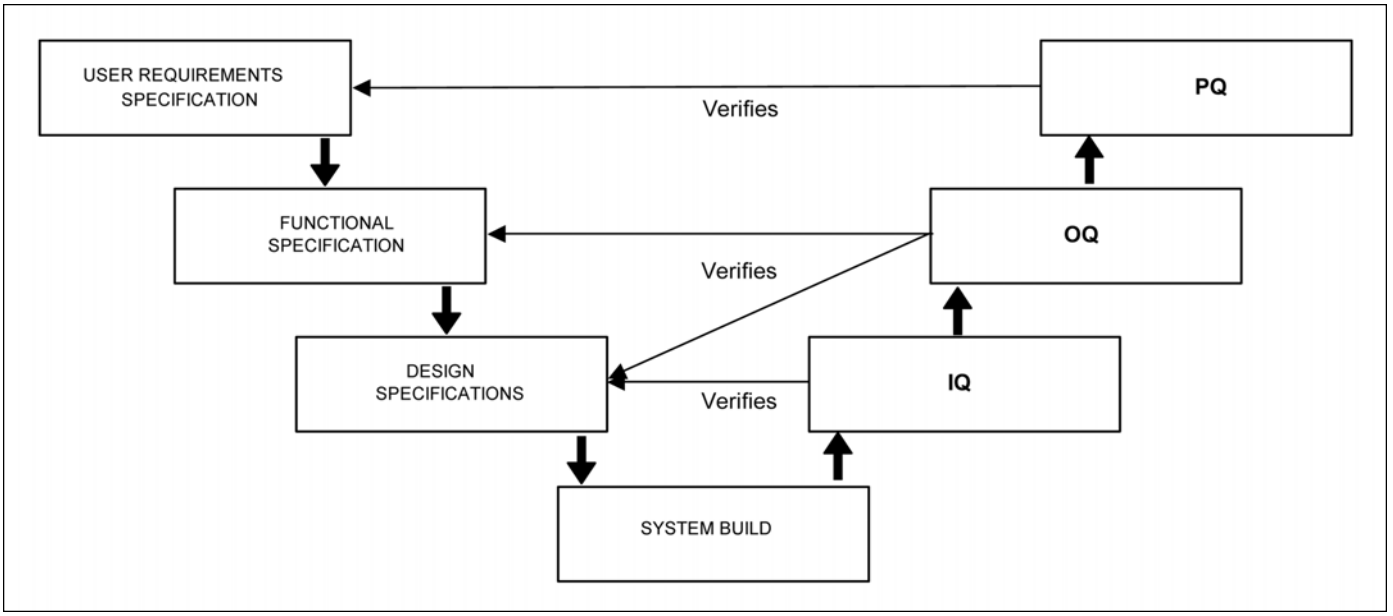

Figure 2. A basic framework for specification and qualification. (This figure is reproduced from GAMP 4).

software, procedures, and reference manuals associated with the Legacy System

- to provide indexes to the documentation set (i.e., by the use of traceability matrices for documents and user requirements)
- to provide a framework to demonstrate regulatory compliance

5 Benefits of Legacy System Validation

Undertaking Legacy System validation has valuable benefits and should not be perceived as having regulatory compliance as its only objective. These benefits include:

- assurance that the system is fit for purpose and relevant to the process that it supports, from both a business perspective and a GxP perspective
- understanding of the actions required to achieve compliance with evolving regulations, e.g., 21 CFR Part 11
- enhanced confidence in the engineering of the Legacy System
- demonstration that users are competent to operate the Legacy System to an appropriate level and are provided with approved procedures
- provision of a baseline from which to manage change control
- potential to reduce system maintenance costs

6 Typical Process for Legacy System Validation

6.1 Scope

It is assumed that a Validation Master Plan (VMP) (see GAMP 4, Appendix M1), or equivalent document, already exists and formally identifies the Legacy Systems under review. As an initial step, this document should be reviewed and updated to ensure that it includes all Legacy Systems and references all Legacy System validation activities.

Figure 1 shows a typical process for Legacy System validation. This process is detailed in Sections 6.2 - 6.9.

6.2 Gap Analysis and Risk Assessment

Once the inventory of a Legacy System is in place, a Gap Analysis can be undertaken, which should be conducted against the V-model, shown in Figure 2 and include a review of the Change Control history for this system (see GAMP 4, Figure 6.2: Basic Framework for Specification and Qualification, and GAMP 4, Appendix M4: Categories of Software and Hardware).

The Gap Analysis should determine the difference between what is in place and what is required to demonstrate that the system has a complete documentation set, is in a state of control, and can be operated and maintained properly. At the same time a Risk Assessment (see GAMP 4, Appendix M3) should be undertaken to determine the criticality of the system to the process (with respect to product efficacy or patient safety).

The Gap Analysis and the Risk Assessment together will help to determine the strategy and the priority in which each system should be addressed for remedial action. High criticality systems with poor compliance will result in a high priority for remedial action, whereas, low criticality systems with poor compliance may fall below the threshold for remedial action, the definition for which shall be described in the VMP. For medium and low GxP criticality systems, it may be acceptable to establish the quality of the documentation set by sampling (or 'spot checking') as recommended in GMA/NAMUR Guideline NE68: Retrospec-

tive Validation of Control Systems.

In the analysis phase, it may be necessary to collect historical evidence of the successful operation of the system (e.g., review of product batch records, event and incident logs) to support the continued use of the system. This approach should be used with caution, as it will be difficult to assure the integrity of historical data unless it is possible to demonstrate good operational control throughout the life of the Legacy System.

If this is part of the Legacy System validation strategy, then this activity should be included in the Validation Plan, as a deliverable, or discussed in the Validation Report, as part of the rationale for not having a complete validation documentation set. For example, if the volume of data is large enough, it may be possible to demonstrate that the system works properly at the boundaries of an alarm range. However, considering the example of a line running at a certain constant speed setting, the limits of the process may not be stretched, and validation testing of the control system at maximum and minimum line speed might be necessary.

The status of the Legacy System supplier should be reviewed to determine whether there are any outstanding issues from any previous audit(s) and, if so, to ensure that all actions are closed out. The review process should also take into account whether there will be a continuing relationship with the supplier. If there is, or because further upgrades are expected, then consideration should be given to when the first, or next, audit should be conducted. Any new audit should encompass a review of the ability of the supplier to meet the requirements of any legislation introduced since the last audit, e.g., 21 CFR Part 11. The result of the supplier review may impact the degree of testing required within the validation program of the Legacy System.

Where no prior supplier audit exists and no further upgrades are expected, the Legacy System is assessed as low risk, or the Legacy System is wholly supported with internal resource, there is little or no value in conducting a supplier audit as part of the Legacy System validation.

6.3 Planning

Once the Gap Analysis and Risk Assessment are complete and a priority has been set, the Validation Plan (VP) for the system can be established. The VMP sets out what activities will be undertaken to validate the system, who will be responsible for the various activities, and in which order those activities will be executed (see GAMP 4 Appendix M1). The VP should, in principle, follow the outline given in the GAMP Appendix, but may be amended to take into account the findings of the Gap Analysis.

At this point, an additional Risk Assessment, which considers the risk category of the identified gaps may further influence the validation tasks (i.e., the gap may be determined to be acceptable). Where gaps exist, reference may be made to existing specifications and historical records (e.g., error logs, change requests), particularly where they add clarity to the scope of the validation activities, provide positive evidence of reliable performance, supplier status etc.

6.4 Specification

The business process or production process being supported by the Legacy System must be understood in detail and will be reflected in the documentation describing the user requirements for the system. For Legacy Systems, this may be included in the Functional Specification (and a URS is not required) or conversely a URS may be in place (and an FS is not required). However, care must be taken to ensure that the current documentation reflects what the system is intended to do at present. It may have changed since first implementation, and indeed, the process this system is supporting also may have changed. (GAMP 4, Appendices D1 and D2 give guidance on the preparation of User Requirements Specifications and Functional Specifications.) The specification document(s) should contain the up-to-date system description covering hardware, software, and the system environment (physical and logical, i.e., operating environment, hardware platform, interfaces), as well as a definition of the functions and facilities provided by the system.

The specification document(s) should be understandable by both the operational users and the technical support staff/system administrators, and be readable, usable, and maintainable.

6.5 Design

Taking into account the criticality of the system determined by the GxP Risk Assessment, the route through the Legacy System validation process is now determined by the availability or not of the design documentation - *Figure 3*.

Where design documentation already exists this should be reviewed and brought up to date to ensure that each element of the Functional Specification is met.

Where design documentation does not exist and the application is not category 5 software, the configuration must be specified. (See GAMP 4 Section 8.1.3 and Appendix M9.)

Where the design documentation does not exist, some part of the application is category 5 software, but no further development is expected or the GxP risk is low, the configuration must be specified, and the system development 'frozen.' (If future code changes are unavoidable, the design documentation must be generated, but can be limited to the scope of the change.)

Where the design documentation does not exist, some part of the application is category 5 software, further development is required and the GxP risk is high, the Design Specification must be reverse engineered from the source code. When such 'reverse engineering' is required, it will be necessary to ensure that:

- The critical algorithms are correct, lacking defects, anomalies, and nonconformance to standards and best practice in the code, which would adversely affect the reengineering of the design documentation.

- The source code and the executable code are the same. (This will largely depend on how well the change control and program promotion procedures are/were controlled in the 'development' and 'live' environments.) (See GAMP 4, Appendix D5).

A properly executed Code Review will give a good indication of the overall integrity and maintainability of the code. The review should result in a report of the findings and any remedial actions that are necessary.

On completion of the Functional Specification and, if necessary, a Code Review, the Design Specifications are required. Guidance on the production of Design Specifications can be found in GAMP 4, Appendix D3 and Appendix D4.

In the event that specifications and source code are absent, the only possibility is to develop a Functional Specification from the process requirements and the system's functionality, as used. However, this in itself is insufficient and must be supported by evidence of reliability in use, such as a formal report of the history, use, maintenance, and change control records of the system, and by functional testing or Operational Qualification (OQ). The continued use of the system will depend on factors, such as the criticality assigned by the Risk Assessment process, and a replacement strategy may need to be considered. To ensure that each element of the user requirements is met by a design, a traceability matrix must be built which will subsequently ensure that each part of the design and each user requirement have a corresponding test. Guidance on Traceability Matrices may be found in GAMP 4, Appendix M5.

Prior to commencing the qualification phase, there is opportunity to review the data held within the system for continued relevance, accuracy, security, and integrity.

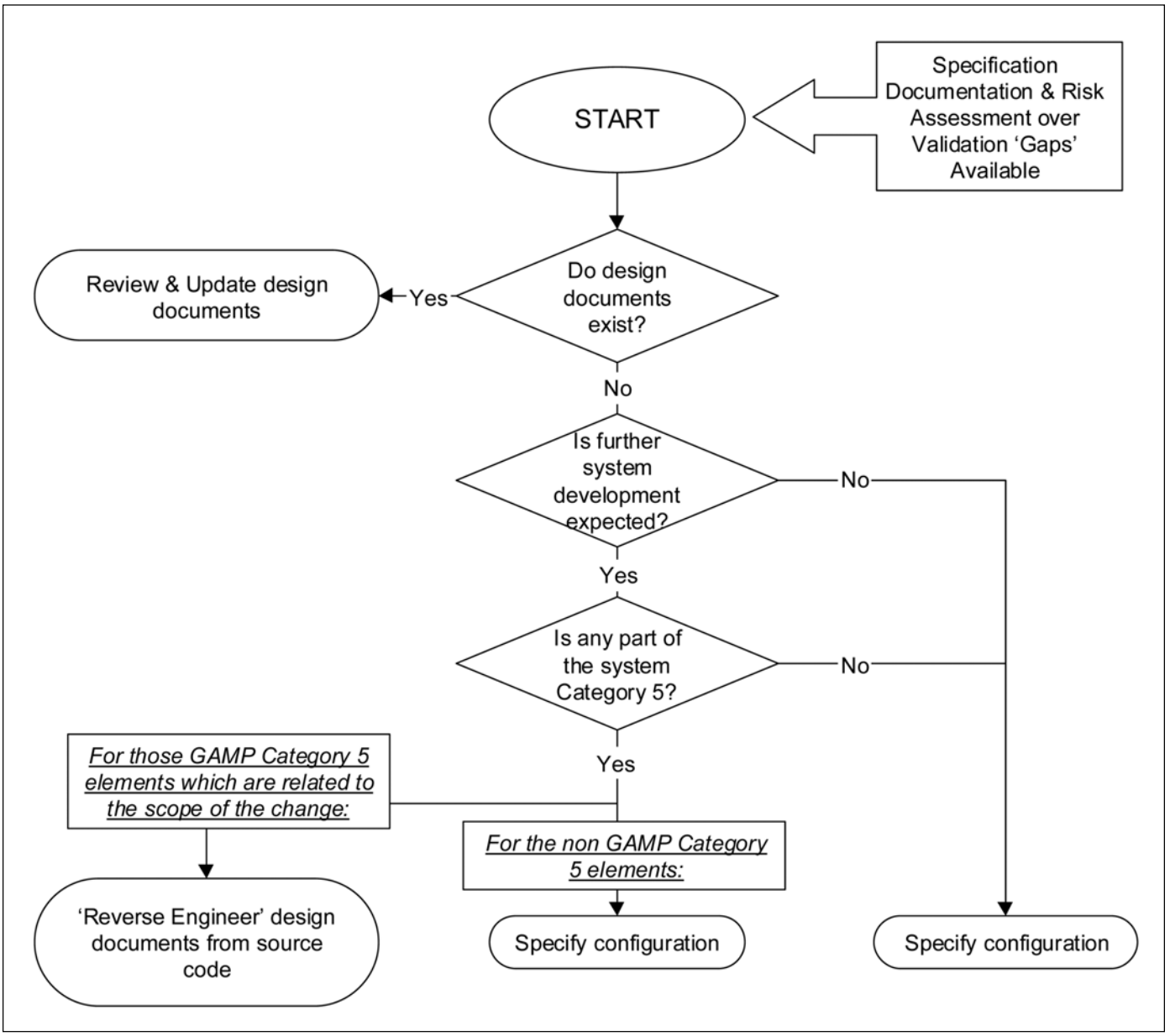

Figure 3. The Legacy System Validation Process.

6.6 Configuration Management

The design level review must address Configuration Management (see GAMP 4, Appendix M9) to ensure that all items subject to configuration control are identified in the design level documents and to provide a baseline for ongoing configuration management.

6.7 Qualification

Using the V-model (see Figure 2) as the framework for the Legacy System validation program, the left hand side of the V is now complete (Specification – Design – Code Review), leading to the right hand side, and the testing phase. Guidance on the scope of the testing phase, in particular Installation and Operational Qualification activities, is given in GAMP 4, Section 6: Validation Overview. Guidance on the details of each test specification may be found in GAMP 4, Appendix D6. It may be possible to review and reuse all or part of the existing Test Specifications. The Test Specification must include tests for all the critical processes in the system and for all anticipated routes through those processes. If any modifications have been made as a result of the review of the specifications or the code, then regression testing must be part of the testing program. If code has been amended as part of the Legacy System validation, then there should be properly documented module and integration testing prior to qualification activities.

When this stage is successfully completed, an appropriate Installation Qualification (IQ) can be executed, which will confirm compliance with the controlling specifications and create the new baseline against which to manage ongoing change control. (This does not require a re-installation of the hardware and software, rather it is a confirmation that what is already in place is what is required.) The IQ will be followed by the Operational Qualification (OQ), which will demonstrate that the system works across its expected operating ranges, and will challenge the system in critical areas, e.g., to demonstrate that it will fail safe when inappropriate entries are made.

The qualification phase also will assure, as with any system, that the procedures for the operation and continuing maintenance of the Legacy Systems are in place to ensure that the system remains in a state of control (see Section 6.9).

Finally, if substantial change has been made to the system as a whole, it may be necessary to confirm its performance in the 'live' environment by executing a Performance Qualification (PQ). All of this testing and qualification must be documented and the results retained as evidence of the success of the testing.

6.8 Reporting

When all of these activities have been completed and the procedures are in place, the validation program will be closed with the preparation of the Final Validation Report, which responds to the Validation Plan. The Final Validation Report should review the results and draw a conclusion on the continued use of the system. (GAMP 4, Appendix M7 gives guidance on preparing the Final Validation Report).

6.9 Maintaining the Validated State

It will now be necessary to ensure that the operational part of the Legacy System's life cycle is maintained in its validated state by ensuring existing operational procedures are kept up to date, clearly defining who is responsible for what.

The system owner is responsible for maintaining the validated state, which involves ensuring that the following operational procedures are in place and followed:

- Operational Plans and Procedures
- Operational Change Control (including data)
- Training
- Security Management
- Problem Management and Resolution
- Performance Monitoring
- Service Level Agreements
- Record Retention, Archiving and Retrieval
- System Management
- Business Continuity Planning
- Backup and Recovery
- Periodic Review and Evaluation
- Configuration Management
- System Retirement

Further details on these topics are provided in GAMP 4, Section 7.11: 'Maintaining the Validated State' and Section 7.11.14: 'System Retirement' and GAMP 4, Appendices O1 to O8.

Appendix O1	Guideline for Periodic Review
Appendix O2	Example Procedure for the Production of a Service Level Agreement
Appendix O3	Guideline for Automated System Security
Appendix O4	Guideline for Operational Change Control
Appendix O5	Guideline for Performance Monitoring
Appendix O6	Guideline for Record Retention, Archiving, and Retrieval
Appendix O7	Guideline for Backup and Recovery of Software and Data
Appendix O8	Guideline for Business Continuity Planning

7 References and Reading List

1. PIC/S Guidance: Good Practices for Computerized Systems in Regulated GxP Environments, PI 011-1; PIC/S August 2003.

2. Good Practice and Compliance for Electronic Records and Signatures, Part 1 - Good Electronic Records Management (GERM) (ISPE/PDA, 2002).

3. Good Practice and Compliance for Electronic Records and Signatures, Part 2 - Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures (ISPE/PDA, 2001).

4. GAMP 4 ISPE (2001), GAMP Guide for Validation of Automated Systems (GAMP 4), International Society for Pharmaceutical Engineering (www.ispe.org).

5. International Standards Organization, BS ISO/IEC 17799:2000, "Information Technology - Code of Practice for Information Security Management."

6. 21 CFR Part 11 - Electronic Records; Electronic Signatures, Department of Food and Drug Administration, US Government, March 20, 1997.

7. VDI/VDE 3517, Part 3 - NAMUR recommendation NE68 Retrospective Validation of Legacy Systems.

8 Acknowledgements

The Legacy Systems Special Interest Group would like to acknowledge the contributions made by the following:

Primary Authors:

Peter Robertson (AstraZeneca)
Kate Samways (KAS Associates)
Rob Stephenson (Pfizer)

Valuable comments were received from:
Rory Budihandojo (GlaxoSmithKline)
Chris Clark (Napp)
Darel Henman (Toyo Business Engineering Systems)
Niels Holger Hansen (NN)
Colin Jones (Conformity)
Tony Margetts (AstraZeneca)
Kathy Pelley (CVE Inc)
Randy Perez (Novartis)
Bob Reba (AAC)
Hellen Rowland Taylor (Purdue Frederick)
Paul Seelig (Merck)
Kate Townsend (Taratec)
Tony Trill (MCA)
Guy Wingate (GlaxoSmithKline)