



GAMP Good Practice Guide

A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems

Second Edition

A leader in providing
Computer Systems
Implementation,
Validation and
Quality Assurance
Services.



SERVICES AVAILABLE

- RISK-BASED LAB RELOCATION
- COMPUTER SYSTEMS VALIDATION
- INSTRUMENT IQ/OQ/PQ SERVICES
- LIFE CYCLE DOCUMENTATION
- LIMS SYSTEM QUALIFICATION
- IT INFRASTRUCTURE
- PROJECT MANAGEMENT

CQV (An Azzur Group Company) provides consulting services to the Life Sciences Industry. We offer system integration, compliance and validation services within the Quality Assurance, Laboratory, Clinical, IT/IM, Business Processes, Manufacturing, Operations, and R&D settings to our pharmaceutical, biotechnology and medical device clients.

With a depth of expertise in all facets of the system life cycle we are able to assist our clients within any phase to reach their goals of running a lean, efficient operation.

“...to achieve success?”

CQV (An Azzur Group Company) takes a holistic approach when working with our clients to provide the best service possible. We work hand in hand with each client to achieve success by ensuring that all goals are met and safe and effective products are delivered.





GAMP Good Practice Guide

A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems

Second Edition

Disclaimer:

This Guide aims to provide a risk-based approach for defining a rational, scalable process to ensure that laboratory computerized systems are fit for intended use and compliant with applicable regulations. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability

In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

© Copyright ISPE 2012. All rights reserved.

No part of this document may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems – without written permission of ISPE.

All trademarks used are acknowledged.

ISBN 978-1-936379-49-1

Preface

The ISPE GAMP® Good Practice Guide: A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems represents a revision of the first edition, ISPE GAMP Good Practice Guide: Validation of Laboratory Computerized Systems and is intended as a supplement to ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems. This Guide provides an overview of the life cycle of laboratory computerized systems, from concept to retirement. It has been updated to align with the concepts and terminology of GAMP® 5 and regulatory and industry developments which focus attention on patient safety, product quality, and data integrity.

This revision:

- Describes a flexible categorization approach consistent with GAMP® 5, based on risks associated with the use of the system to support the relevant business process
- Applies the GAMP® 5 specification and verification approach to laboratory computerized systems
- Emphasizes the importance of leveraging supplier documentation and knowledge to avoid unnecessary duplication of efforts

This Guide provides direction for identifying, securing, and managing critical electronic records involved in regulated business decisions, consistent with recent regulatory guidance.

This Guide has been designed so that it may be used in conjunction with GAMP® 5 and other ISPE publications, such as the ISPE Baseline® Guides.

Appendices to this revision include examples for:

- Simple systems (e.g., pH meter, balance)
- Medium systems (e.g., HPLC)
- Complex systems

Additional appendices address concerns related to:

- Data integrity
- Defining electronic records and raw data
- Security management
- System interfacing considerations
- Robotics systems

The ISPE GAMP Community of Practice (COP) Laboratory Systems Special Interest Group (SIG) was asked to revise this Guide. The team consisted of representatives from regulated companies, Contract Research Organizations (CROs), suppliers of laboratory computerized systems, and independent consultants.

Acknowledgements

The production of the ISPE GAMP Good Practice Guide: Risk-Based Approach to GxP Compliant Laboratory Computerized Systems was initiated by the Laboratory Systems SIG at the request of the GAMP Council.

The following members of the GAMP COP Laboratory Systems SIG worked on one or more sections of this Guide and volunteered countless hours to attend meetings and review the many drafts, which were produced over a two year period. It has been informative and satisfying to work with such a dedicated group of professionals on this project.

Chairs

Lorrie Vuolo-Schuessler	GlaxoSmithKline	USA
Mark Newton	Eli Lilly and Company	USA

SIG Members

Rachel Adler	Janssen Pharmaceutical Companies of J&J	USA
Peter Brandstetter	Arcondis GmbH	Austria
David M. Dube	AVEO Pharmaceuticals Inc.	USA
Karen Evans	GlaxoSmithKline	USA
Craig R. Johnson	Amgen Inc.	USA
Carol Lee	JRF America	USA
Kiet T. Luong	GlaxoSmithKline	USA
Bob McDowall	McDowall Consulting	United Kingdom
Judith S. Samardelis	MedImmune Inc.	USA
Paul Smith	Agilent Technologies	United Kingdom
Peter Ward	IDBS	United Kingdom
Christopher H. White	Eisai Inc.	USA

GAMP Council Sponsor

Winnie Cappucci	Bayer Healthcare (retired)	USA
-----------------	----------------------------	-----

The GAMP Laboratory Systems SIG would like to acknowledge the support of their direct management and companies in this endeavor.

The GAMP Laboratory Systems SIG would like to express their thanks to the following who facilitated alignment of this Guide with USP <1058>, through valuable discussion, advice, and review comments:

Christopher Burgess	Burgess Analytical Consultancy Limited	United Kingdom
Horacio Pappa, PhD	US Pharmacopeial Convention	USA

The GAMP Laboratory Systems SIG would like to express their thanks to the following for their contributions:

Frank Behnisch	CSL Behring GmbH and GAMP DACH	Germany
Shelley Gutt	Covance, Inc.	USA
Heather Longden	Waters Corporation	United Kingdom
Rene Schuermann	Mettler Toledo	Switzerland
Marcus Zeitz	Novartis Pharma AG	Switzerland

Particular thanks go to the GAMP COP Editorial Review Board for their review and comment:

Chris Clark (Chair)	Napp Pharmaceuticals Limited	United Kingdom
Winnie Cappucci	Bayer Healthcare (retired)	USA
Gail Evans	ISPE	United Kingdom
Colin Jones	Conformity Limited	United Kingdom
Randy Perez	Novartis Pharmaceuticals	USA
Sion Wyn	Conformity Limited	United Kingdom

The Leaders of the GAMP Laboratory Systems SIG wish to thank GAMP Council, GAMP Americas Steering Committee, and the Guidance Documents Executive Committee (GDEC) for their contributions and commitment throughout the production of this Guide.



**Connecting a World of
Pharmaceutical Knowledge**

ISPE Headquarters

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

ISPE Asia Pacific Office

73 Bukit Timah Road, #04-01 Rex House, Singapore 229832
Tel: +65-6496-5502, Fax: +65-6336-6449

ISPE China Office

Suite 2302, Wise Logic International Center
No. 66 North Shan Xi Road, Shanghai, China 200041
Tel +86-21-5116-0265, Fax +86-21-5116-0260

ISPE European Office

Avenue de Tervueren, 300, B-1150 Brussels, Belgium
Tel: +32-2-743-4422, Fax: +32-2-743-1550

www.ISPE.org

Table of Contents

1	Introduction	7
1.1	Rationale.....	7
1.2	New and Revised Material	8
1.3	Purpose.....	8
1.4	Scope.....	9
1.5	Business Benefits	10
1.6	Structure	10
2	Key Concepts	13
2.1	Key Concepts.....	13
2.2	Key Terms	15
3	Life Cycle Approach	19
3.1	Computerized System Life Cycle.....	19
3.2	Specification and Verification	20
3.3	Computerized System Validation Framework.....	21
4	Life Cycle Phases	23
4.1	Concept.....	23
4.2	Project.....	24
4.3	Operation	30
4.4	Retirement	38
5	Quality Risk Management	43
5.1	Science-Based Quality Risk Management.....	43
5.2	Quality Risk Management Process.....	44
5.3	Initial Risk Assessment	44
5.4	Implement and Verify Appropriate Controls	47
5.5	Review Risks and Monitor Controls	48
6	Regulated Organization Activities.....	49
6.1	Governance for Achieving Compliance.....	49
6.2	System Specific Activities	50
7	Supplier Relationships	53
7.1	Leveraging Supplier Knowledge and Documentation	54
7.2	Supplier Assessment	54
8	Appendix 1 – Categories of Software	57
9	Appendix 2 – System Description	61
10	Appendix 3 – Data Integrity	67
10.1	Introduction	67
10.2	Critical Success Factors	67

11	Appendix 4 – Simple Systems	71
11.1	Generic Activities for Simple Systems	71
11.2	Example 1 – Analytical Balance	75
11.3	Example 2 – Ph Meter	78
11.4	Example 3 – Electronic Pipette	81
12	Appendix 5 – Medium Systems	83
12.1	Scope of Activities When Connected to an External System	83
12.2	Generic Activities for Medium Systems	84
13	Appendix 6 – Complex Systems	91
13.1	System Architecture	91
13.2	Multidisciplinary Approach to Validation	92
13.3	Order of Validation Activities	92
13.4	Validation Activities	92
14	Appendix 7 – System Interfacing Considerations	107
14.1	LIMS Overview	107
14.2	ELN Overview	107
14.3	Aspects to Consider	108
14.4	ELN/LIMS Interface Verification Approach	113
15	Appendix 8 – Robotics Systems	119
15.1	Overview	119
15.2	Planning Considerations	119
15.3	Risk Management Considerations	121
15.4	Verification Activities for Robotics Systems	122
16	Appendix 9 – Defining Electronic Records and Raw Data	129
16.1	Regulatory Rationale for Defining Records and Raw Data	129
16.2	Illustrative Example: Defining Raw Data/Electronic Records for a Chromatography Data System (CDS)	131
17	Appendix 10 – Security Management for Laboratory Computerized Systems	135
17.1	Introduction	135
18	Appendix 11 – Supplier Documentation and Services	139
18.1	System Development by the Supplier	139
18.2	Supplier Assessment	139
18.3	Supplier Good Practices	142
19	Appendix 12 – References	145
20	Appendix 13 – Glossary	147
20.1	Acronyms and Abbreviations	147
20.2	Definitions	149

1 Introduction

This Guide is a revision of the first edition of the ISPE GAMP Good Practice Guide (GPG) on this topic: GAMP GPG: Validation of Laboratory Computerized Systems. It has been updated to align with the concepts and terminology of GAMP® 5 [1], and recent regulatory and industry developments. These developments focus attention on patient safety, product quality, and data integrity.

GAMP® 5 and associated GPGs aim to provide guidance to achieve computerized systems that are fit for intended use and meet current GxP regulatory requirements by building upon existing industry good practice in an efficient and effective manner.

The approach and terminology is also harmonized with the following industry guidance:

- International Conference on Harmonization (ICH) Guidance including Q8, Q9, and Q10 [2, 3, 4]
- American Society for Testing and Materials (ASTM) Standard E2500, Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment [5]

The approach is intended to align with the proposed update to United States Pharmacopoeia General Chapter, <1058> Analytical Instrument Qualification underway at time of publication [6].

For brevity, throughout this Guide, the term “system” refers to “laboratory computerized system” unless otherwise indicated.

GAMP is an ISPE Community of Practice. For further information, see www.ispe.org [7].

1.1 Rationale

The automation of laboratory testing and data management operations is increasing in sophistication and complexity. Widespread reliance on these technologies, along with their potential impact on data integrity, has brought an increased focus on the importance of appropriate selection, implementation, control, and maintenance of laboratory computerized systems.

Due to the wide diversity of systems, a single prescriptive approach would be neither practical nor cost-effective. For example, a High Performance Liquid Chromatograph (HPLC) with a Photo Diode Array (PDA) detector is much more complex than a pH meter, and will require a correspondingly more detailed and complex implementation, control, and maintenance approach.

The aim is to achieve compliance, efficiency, and effectiveness – within a reasonable budget and timeline – for a wide variety of systems. It is recognized that many laboratory computerized systems are now based on configurable packages, many of them networked.

Poor management of laboratory computerized system acquisition, implementation, and operation may result in:

- Failing to meet process and user requirements
- Unacceptable cost or time overruns
- Risk of non-compliance
- Data integrity issues

This Guide seeks to develop a rational approach to laboratory computerized system specification, verification, and implementation by:

- Examining the system life cycle and its applicability for most laboratory computerized systems
- Identifying characteristics that distinguish various types of laboratory computerized systems
- Developing a rationale for scaling activities and effort based upon risk, complexity, and novelty
- Defining a strategy for supplier assessments, and the effective leveraging of supplier knowledge, experience, and documentation
- Applying the GAMP® 5 [1] Quality Risk Management (QRM) approach
- Defining necessary operational and maintenance activities
- Recommending an approach to system retirement
- Leveraging deliverables and activities for very similar or identical systems

This flexible approach is aligned with industry trends and drivers and supports rapid implementation of low risk and less complex systems. The approach requires better knowledge of the business process and intended system use, but results in greater efficiency and productivity, and a focus on the most critical activities. As a Subject Matter Expert (SME), the laboratory scientist needs to understand the business process and the risks to the integrity of their data based upon intended use.

1.2 New and Revised Material

The previous edition of this Good Practice Guide classified laboratory computerized systems into discrete sub-categories based upon a set of criteria, such as configuration, interfaces, data processing, and data storage. This revision describes a flexible categorization approach consistent with GAMP® 5 [1], and based on the risks associated with the use of the system to support the relevant business process.

This revision applies the GAMP® 5 [1] specification and verification approach to laboratory computerized systems.

This revision emphasizes the importance of leveraging supplier documentation and knowledge, whenever possible, to avoid unnecessary duplication of efforts.

1.3 Purpose

As a Good Practice Guide supporting GAMP® 5 [1] this Guide provides a harmonized overview of the life cycle of laboratory computerized systems, from concept to retirement.

This Guide is intended for use by regulated organizations, suppliers, and regulators. The intended audience for this Guide includes laboratory, quality, and computer validation professionals responsible for defining and managing laboratory computerized systems in regulated life science industries. Information Technology (IT) support personnel, management, and laboratory systems users (who are an integral part of the process), software developers, and suppliers of laboratory computerized systems are also expected to find benefit in using this Guide. Suppliers include providers of software, hardware, analytical instrumentation, system integration services, and IT support services, both internal and external to the regulated organization.

This Guide builds upon the framework presented in GAMP® 5 [1] to provide a risk-based approach for defining a rational, scalable approach to ensure that laboratory computerized systems are fit for intended use and compliant with applicable regulations. The focus throughout is on *data integrity, product quality, and patient safety*.

GAMP documents are guides and not standards. It is the responsibility of regulated organizations to establish policies and procedures to meet applicable regulatory requirements. Consequently, it is inappropriate for suppliers of products to claim that they are GAMP certified, approved, or compliant.

It is recognized that there are acceptable approaches other than those described in this Guide. *The Guide is not intended to place any constraints on innovation and development of new concepts and technologies.*

1.4 Scope

This Guide addresses laboratory computerized systems used within the regulated life science industries, including pharmaceutical, biological, and medical devices that are subject to:

1. Good Manufacturing Practice (GMP)
2. Good Laboratory Practice (GLP)
3. Good Clinical Practice (GCP)
4. Medical Device Regulations (with the exception of software embedded within medical devices)

These are collectively known as GxP regulations.

For the purposes of this Guide, the term *laboratory computerized system* refers to systems supporting a wide range of laboratory processes, including analysis of drug products, in-process materials, Active Pharmaceutical Ingredient (API), excipients, environmental samples, clinical samples, or toxicology samples. These may include:

- Configured and non-configured products
- Custom applications
- Analytical and other instruments, i.e., devices used to carry out a measurement

Systems within the scope of this Guide support a wide range of processes, including but not limited to analysis of drug products, in process materials, Active Pharmaceutical Ingredient (API), excipients, environmental samples, clinical samples, or toxicology samples.

Not all the activities defined in this Guide will apply to every system. The scalable approach enables regulated organizations to select the appropriate life cycle activities based upon risk.

IT systems, such as Laboratory Information Management Systems (LIMS), are not specifically addressed since the approach described in GAMP® 5 [1] is directly applicable. Equipment interfaced to such systems is; however, addressed (see Appendix 9). This Guide does not cover infrastructure aspects, except in reference to specific issues related to laboratory systems.

1.5 Business Benefits

There are major business benefits in having a defined process that delivers systems that are fit for intended use, on time, and within budget. Systems that are well defined and specified are easier to support and maintain, resulting in less downtime and lower maintenance costs.

Specific benefits to both regulated organizations and suppliers include:

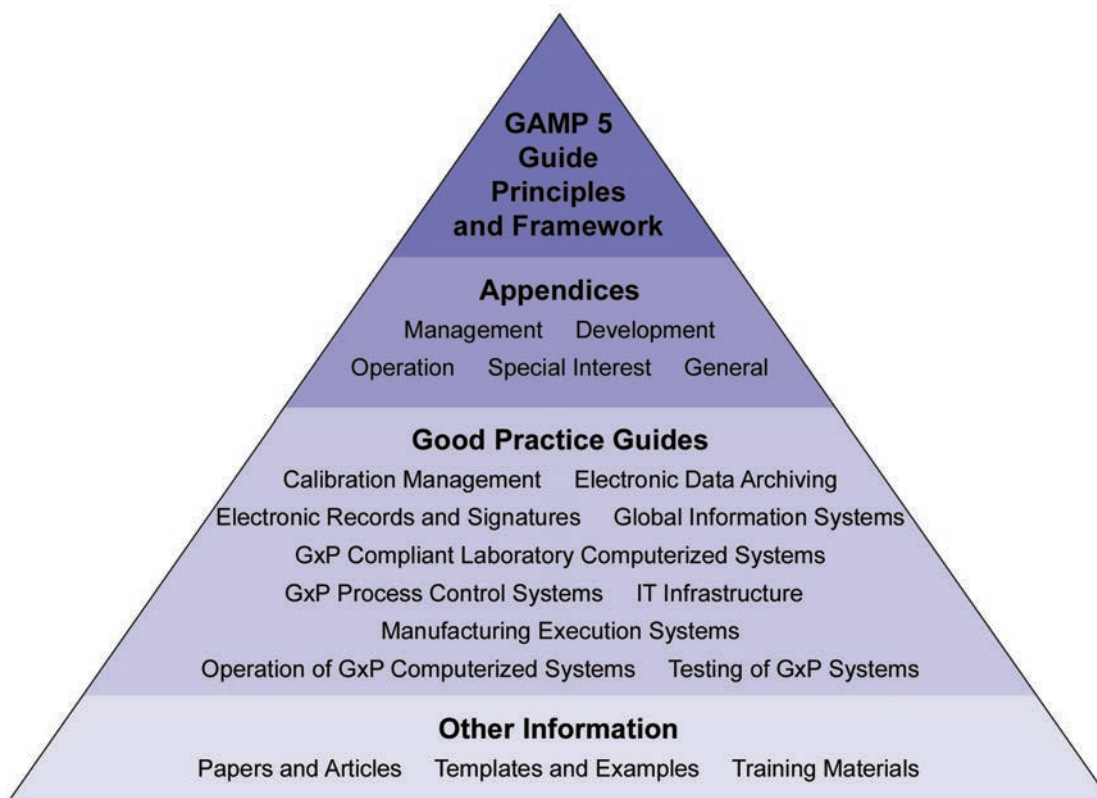
- Reduction of cost and time taken to achieve and maintain compliance
- Early defect identification and resolution leading to reduced impact on cost and schedule
- Cost effective operation and maintenance
- Effective change management and process for continual improvement
- Enabling of innovation and adoption of new technology
- Providing frameworks for user/supplier co-operation
- Assisting suppliers to produce required documentation
- Promotion of common, consistent, system life cycle, language, and terminology
- Providing practical guidelines and examples
- Promoting pragmatic interpretation of regulations

1.6 Structure

1.6.1 Overview of GAMP Documentation Structure

This Good Practice Guide forms part of a family of documents that together provide a powerful and comprehensive body of knowledge covering all aspects of computerized systems good practice and compliance.

Figure 1.1: GAMP Documentation Structure



1.6.2 Structure of this Guide

The main body introduction covers the rationale, new and revised material, purpose, scope, business benefits, and structure of this GAMP documentation. Subsequent sections of the main body cover the topics:

- Key concepts
- Life cycle approach
- Life cycle phases
- Quality Risk Management (QRM)
- Regulated organization activities
- Supplier activities

Appendices to this revision include examples for simple, medium, and complex systems. Additional appendices address concerns related to data integrity, data security system interfaces, and robotics systems

2 Key Concepts

2.1 Key Concepts

The following key concepts – aligned with GAMP® 5 [1] – are applied throughout this Guide:

1. Product and process understanding
2. Life cycle approach within a Quality Management System (QMS)
3. Scalable system life cycle and life cycle activities
4. Science-based quality risk management
5. Leveraging supplier involvement
6. Calibration of laboratory systems

2.1.1 *Product and Process Understanding*

An understanding of the supported process, intended business use, and data produced is fundamental in determining the system requirements. Consideration also should be given to decisions which may be made from the information produced by these systems. For laboratory computerized systems, efforts to ensure fitness for intended use should focus on those aspects that are critical to data integrity, product quality, and patient safety. These critical aspects should be identified, specified, and verified.

The extent and detail of the requirements should be commensurate with the associated risk, complexity, and novelty of the system. Incomplete or inaccurate process understanding hinders effective and efficient compliance and achievement of business benefit. Product and process understanding is the basis for making science- and risk-based decisions to ensure that the system is fit for its intended use.

Laboratory computerized systems may be configured and modified by the end-user of the system. A particular implementation of the same laboratory computerized system product or package may require additional scrutiny or control based on the use of the system and nature of the data.

2.1.2 *Life Cycle Approach within a Quality Management System*

Adopting a complete computerized system life cycle entails defining activities in a systematic way from system conception to retirement. This enables management control and a consistent approach across systems. The life cycle should form an intrinsic part of the organization's Quality Management System (QMS), which should be maintained as new ways of working are developed.

A suitable life cycle, properly applied, enables the assurance of quality and fitness for intended use, and assists with achieving and maintaining compliance with regulatory requirements. A well-managed and understood life cycle facilitates adoption of a Quality by Design (QbD) approach.

Many laboratory computerized systems are standard or configurable products consisting of closely integrated hardware and software that are best verified and challenged as an integrated unit. For example, it would be impractical to separately test a Near Infrared (NIR) spectrophotometer's hardware and software.

A suitable life cycle should be selected based on risk, complexity, novelty, and the nature of the system components (e.g., non-configured, configured, or custom). The Guide applies a general approach for achieving computerized system compliance and fitness for intended use within the system life cycle. Specification activities have equivalent verification steps to determine whether specifications have been met. A hierarchy of specifications may be required for larger systems, while specifications may be combined for smaller, simpler, systems or systems classed as low risk. Specifications should be addressed by appropriate verification steps.

For many laboratory systems, operational phase aspects and controls are equally important in achieving fitness for intended use and managing risks to data integrity.

2.1.3 Scalable Life Cycle Activities

Life cycle activities should be scaled according to:

- System impact on patient safety, product quality, and data integrity (risk assessment)
- System complexity and novelty (architecture and system components)
- Outcome of supplier assessment (supplier capability)

Business impact also may influence the scaling of life cycle activities.

2.1.4 Science-Based Quality Risk Management

Quality risk management is a systematic process for the assessment, control, and communication and review of risks managed throughout the life cycle of the laboratory computerized system.

Application of quality risk management enables effort to be focused on critical aspects of a system.

Quality risk management should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity. Qualitative and quantitative techniques may be used to identify and manage risks. Controls are developed to reduce risks to an acceptable level. Implemented controls are monitored during operation to ensure ongoing effectiveness. Risk mitigation decisions should be documented. The strategies to manage risk may include procedural controls, technical controls, and validation controls.

2.1.5 Leveraging Supplier Involvement

Organizations should seek to maximize the use of supplier information and supplier involvement throughout the system life cycle in order to leverage knowledge, experience, and documentation. The limits and acceptance criteria applied to any testing performed by the supplier specifically for the user should be approved. An organization also can standardize the data repository to simplify the scope and data handling portion of the instrument's life cycle. The supplier can support this goal by using a well defined export/import file structure.

For example, the user may acquire documentation from the supplier to supplement their own:

- User requirements
- Risk assessments
- System configuration
- Testing, support, and maintenance

As there is a continuum of system complexity, configuration, and customization, there is a range of supplier involvement in providing system information. The process owner is ultimately responsible for compliance.

Planning should determine how best to use supplier documentation, including product data sheets and specifications, and existing test documentation (e.g., test scenarios, executed test scripts, testing templates) to avoid wasted effort and duplication. Justification for the use of supplier documentation depends upon the satisfactory outcome of supplier assessments, which may include on-site supplier audits or supplier certifications. Documentation should be assessed for suitability, accuracy, and completeness through traceability and risk assessment. There should be flexibility regarding acceptable format and structure.

Supplier information for maintenance and calibration activities also may be leveraged by the regulated organizations to document system maintenance. It is important to ensure that control is maintained during preventive maintenance or operational verification activities, especially if performed by a supplier on the production system.

For further information on supplier assessment, see Appendix 11 and GAMP® 5 [1].

2.1.6 Calibration of Laboratory Systems

For many laboratory computerized systems, calibration is a fundamental part of the activities to ensure fitness for intended use and that the data is reliable, accurate, and traceable. Regulated organizations should ensure that a consistent approach to calibration is applied.

Various regulations (such as CFR 21.160(b)(4) [8]) include requirements for documented calibration procedures for items such as instruments, apparatus, gauges, and recording devices.

The ISPE GAMP Good Practice Guide: A Risk-Based Approach to Calibration Management [9] describes the principles to be applied when determining the steps to calibration versus system suitability testing.

There is a correlation between the quality of the calibration and the quality of the result, and is therefore an important aspect for compliant laboratory computerized systems.

Calibration establishes the relationship between the values of an instrument and a known traceable standard, but calibration alone is not sufficient, as it focuses only on the instrument and does not consider data integrity, intended use, additional verification activities or other required controls. Calibration should be completed before starting any functional or system testing, which relies upon instrumentation for an accurate reading.

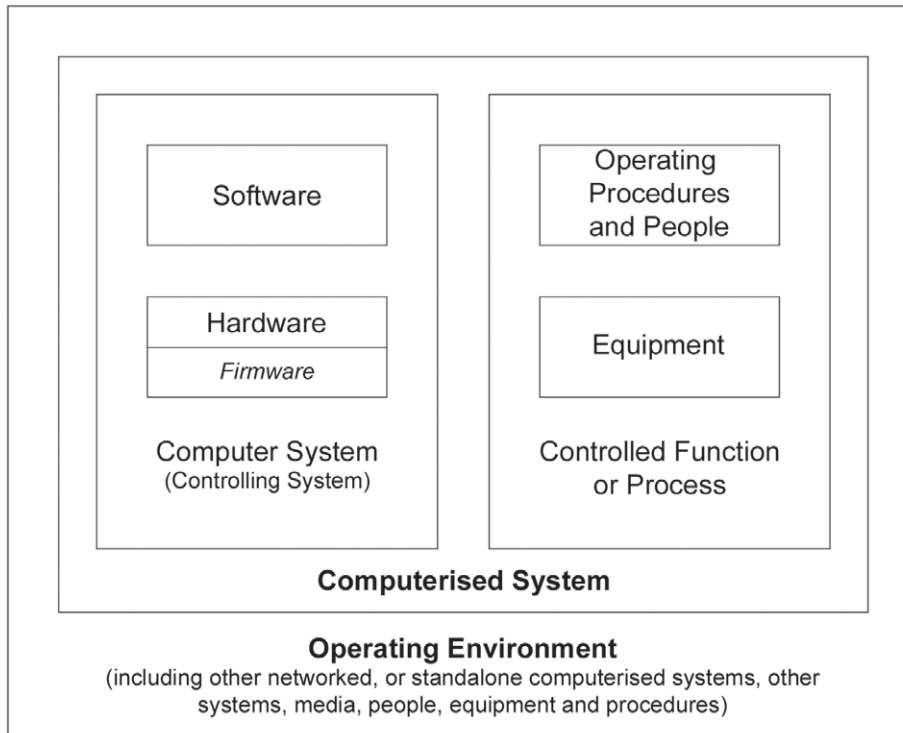
2.2 Key Terms

Calibration

The set of operations which establish, under specified conditions, the relationship between values indicated by a measuring instrument or measuring system, or values represented by a material measure or a reference material, and the corresponding values of a quantity realized by a reference standard. (ISO 10012 [10])

Computerized System

The computerized system consists of the hardware, software, and network components, together with the controlled functions and associated documentation. (GAMP® 5 [1]) (For further information on network components, see the GAMP Good Practice Guide: IT Infrastructure Control and Compliance [11]).

Figure 2.1: Computerized System – from PIC/S Guidance

PIC/S Good Practices for Computerized Systems in Regulated "GXP" Environment" (PI 011 [12]).

GxP Compliance

Meeting all applicable pharmaceutical and associated life-science regulatory requirements.

GxP Regulated Computerized System

Computerized systems that are subject to GxP regulations. The regulated organization must ensure that such systems comply with the appropriate regulations.

GxP Regulation

The underlying international pharmaceutical requirements, such as those set forth in the US FD&C Act, US PHS Act, FDA regulations, EU Directives, Japanese regulations, or other applicable national legislation or regulations under which an organization operates.

These include, but are not limited to (further descriptions provided in Glossary):

- GMP
- GCP
- GLP
- GDP
- Good Quality Practice (GQP)

- Good Pharmacovigilance Practice
- Medical Device Regulations
- Prescription Drug Marketing Act (PDMA)

Process Owner

The person ultimately responsible for the business process or processes being managed. This person is usually the head of the functional unit or department using that system although the role should be based on specific knowledge of the process rather than position in the organization. The process owner is responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable Standard Operating Procedures (SOPs) throughout its useful life. Responsibility for control of system access should be agreed between process and system owner. In some cases, the process owner also may be the system owner.

(**Note:** ownership of the data held on a system should be defined and typically belongs to the process owner).

Quality Management System (QMS)

Management system to direct and control an organization with regard to quality. (International Organization for Standardization (ISO)).

(This is equivalent to **quality system** as defined in ICH Q10 [4].)

Subject Matter Expert (SME)

Those individuals with specific expertise in a particular area or field. SMEs should take the lead role in the verification of computerized systems. SME responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results. (ASTM E2500 [5])

System Owner

The person ultimately responsible for the availability, support and maintenance of a system, and for the security of the data residing on that system. This person is usually the head of the department responsible for system support and maintenance although the role should be based on specific knowledge of the system rather than position in the organization. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. Responsibility for control of system access should be agreed between process and system owner. In some cases, the system owner also may be the process owner.

3 Life Cycle Approach

Compliance with regulatory requirements and fitness for intended use may be achieved by adopting a life cycle approach following good practice as defined in this Guide. A life cycle approach entails defining and performing activities in a systematic way from conception, implementation, release, and operation, and retirement.

The computerized system life cycle approach defined in GAMP® 5 [1] is applicable to laboratory computerized systems and should be applied.

Life cycle activities should be scaled according to:

- System impact on patient safety, product quality, and data integrity (risk assessment)
- System complexity and novelty (architecture and categorization of system components)
- Outcome of supplier assessment (supplier capability)

Scalability involves tailoring the system life cycle by selecting the appropriate life cycle activities, and choosing the appropriate extent, effort, rigor, and level of documentation for these activities.

Many computerized laboratory systems comprise commercially available software products running on standard hardware components, or may involve the configuration of commercially available software products running on standard hardware components. The life cycle activities selected should reflect this (see Appendix 1).

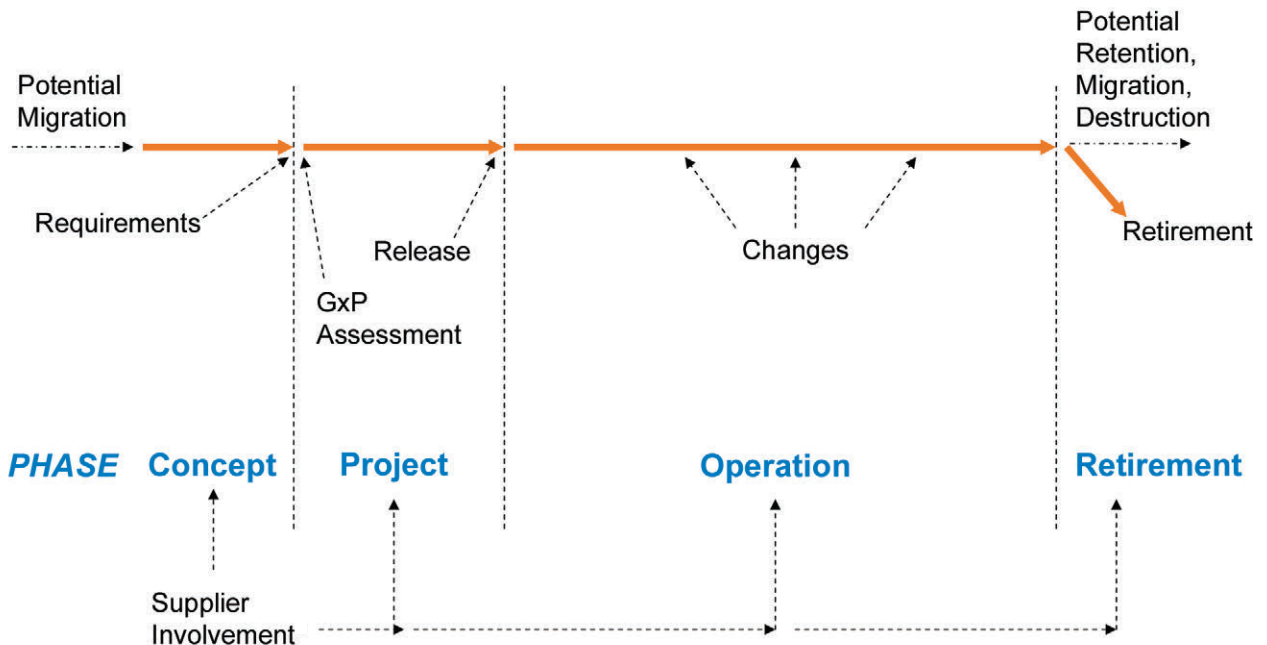
3.1 Computerized System Life Cycle

The life cycle for any system including laboratory computerized systems consists of four major phases:

- Concept
- Project
- Operation
- Retirement

Life cycle phases are shown in Figure 3.1.

Figure 3.1: Life Cycle Phases

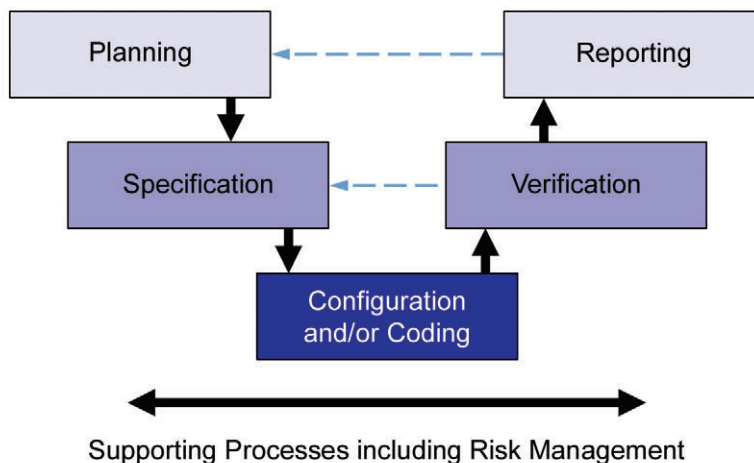


3.2 Specification and Verification

Figure 3.2 depicts the general approach to achieve compliance and fitness for intended use for laboratory computerized systems.

As shown, the specification activities have equivalent verification steps to determine whether the specification has been met. A hierarchy of specifications may be required for complex systems, while specifications may be combined for simple or low risk systems. Specifications should be addressed by appropriate verification steps.

Figure 3.2: A General Approach for Achieving Compliance and Fitness for Intended Use



3.3 Computerized System Validation Framework

Quality risk management should be central to the approach to focus the effort on the laboratory computerized systems and functions where failures would have the highest risk to patient safety, product quality, and data integrity. This approach will vary depending on the risk posed by the criticality, complexity, and novelty of the system. It is recognized that other approaches and models may be used to achieve compliance and fitness for use, but risk should be used to focus the associated activities.

4 Life Cycle Phases

This section further describes the phases of the computerized system life cycle introduced in Section 3.1 of this Guide.

The specific terminology used to describe life cycle activities and deliverables varies from organization to organization and from system type to system type. This Guide does not intend to prescribe any one set of terms to the exclusion of others.

Table 4.1 shows how qualification terminology, as traditionally used, relates to the activities described in this Guide, which is aligned to GAMP® 5 [1]. This will assist readers who use this terminology with the application of this Guide.

Whatever terminology is used for verification activity, the overriding requirement is that the regulated organization can demonstrate that the system is compliant and fit for intended use.

Table 4.1: Relationship between Traditional Qualification Terminology and GAMP® 5 Activities

Traditional Term	Description	GAMP® 5 Verification Activity
Design Qualification	Documented verification that the proposed design of facilities, systems, and equipment is suitable for the intended purpose.	Design Review
Installation Qualification	Documented verification that a system is installed according to written and pre-approved specifications.	Checking, testing, or other verification to demonstrate correct: <ul style="list-style-type: none">• installation of software and hardware• configuration of software and hardware
Operational Qualification	Documented verification that a system operates according to written and pre-approved specifications throughout specified operating ranges.	Testing or other verification of the system against specifications to demonstrate correct operation of functionality that supports the specific business process throughout all specified operating ranges.
Performance Qualification	Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and pre-approved specifications, within the scope of the business process and operating environment.	Testing or other verification of the system to demonstrate fitness for intended use and to allow acceptance of the system against specified requirements.

4.1 Concept

During the concept phase, business needs, processes, and potential solutions are assessed. Typically, initial requirements are developed within this phase.

From an initial understanding of scope, costs, and benefits, a decision is made on whether to proceed to the project phase. Generally, these activities are outside the scope of GAMP.

4.2 Project

The project phase involves planning, supplier assessment and selection, various levels of specification, configuration (or coding for custom applications), and verification leading to acceptance and release for operation. Risk management is applied to identify risks and to remove or reduce them to an acceptable level.

The Project phase contains the following stages:

- Planning
- Specification, configuration, and coding
- Verification
- Reporting and release

Activities conducted during this phase should be scaled in proportion to risks to data integrity, product quality, and patient safety, including:

- Technical complexity of the system
- The degree of configuration
- The intended use of the system, i.e., the business process supported by the laboratory computerized system
- The organization's experience with the technology and supplier

For laboratory computerized systems, it is appropriate to reference/rely on activities performed by the suppliers, subject to satisfactory supplier assessment and control measures.

A GxP assessment should be performed early in this phase to determine if a system is regulated, and if so, which specific regulations apply and to which parts of the system they are applicable. It may be appropriate to base the GxP assessment on the results of a previous system assessment provided the regulated organization has an established procedure. For multiple identical laboratory computerized systems, this information may be part of a template or a generic document.

The strategy for achieving and maintaining compliance and fitness for intended use should be commensurate with risk, complexity, and novelty. Strategies for compliance should be formally planned and documented for complex analytical instruments, but an approach using procedural documents or SOPs may be appropriate for simple or low risk systems.

There may be multiple installations of the same laboratory computerized system within a facility. It may not be necessary to perform repeated assessments of each system when they are configured in the same manner and have the same intended use. A full assessment of the system features may be performed on one system. Subsequent installations of the same system may rely on the initial assessment of functionality, supplemented by confirmation that the configuration remains the same and the systems have been installed correctly.

4.2.1 Planning

A computerized system validation plan should be produced for most regulated laboratory computerized systems, focusing on aspects related to patient safety, product quality, and data integrity.

It should define the life cycle, identify measures for success, and clearly define criteria for final acceptance and release of the system.

(The term computerized system validation plan is used for consistency with GAMP® 5 [1], but it is recognized that some companies use alternative terminology, including validation protocol, compliance plan, or quality plan).

Activities should be scaled in response to the risk factors identified during initial risk assessment.

A generic or common plan may be used for very similar or identical systems (e.g., all Ultraviolet (UV) spectrophotometers for similar use and in a similar setting).

The plan should define:

- What activities are required
- How those activities will be performed
- Who is responsible
- Their products (deliverables)
- Requirements for acceptance
- How compliance will be maintained for the lifetime of the system

Planning should commence as early as possible, ideally no later than development of the User Requirements Specification (URS). The plan may require modification during the project if there is a significant change in strategy or scope following initial approval, in which case project change management should be applied and the plan updated accordingly.

Since the supplier may provide deliverables or directly support some activities, planning provides the opportunity to decide how best to leverage supplier activities and documentation to avoid unnecessary duplication.

The plan should be maintained under change management. The plan should be developed with input from the supplier, users, quality control and quality assurance, system support managers, and the sponsor or business entity (e.g., process owner). Appropriate levels of management should approve the plan to assure adequate support and sponsorship.

Appendix M1 of GAMP® 5 [1] gives detailed guidance on computerized system validation planning, and Section 5.3 of that appendix gives guidance on the suggested contents of the plan.

Rigorous planning allows management to anticipate the needs of the project, and establish a baseline to track progress. Maintaining control of a project affects its economics and ultimately its regulatory compliance and fitness for intended use. For example, in case of financial difficulties, it may be possible to reduce the scope in an attempt to finish on time and within budget. If cut too severely, the final system may be unfit for its intended use.

The need for a separate project plan depends upon the:

- The nature of the system
- The scale and scope of the project
- Number of people involved in implementation

Project plans may be incorporated into computerized system validation plans for less complex projects. If the project plan is produced separately, it should explicitly provide for the activities and deliverables that will be managed under the validation plan. Deliverables should be defined in either the project plan or the validation plan and where necessary cross-referenced. Early in a project, planning can be expected to undergo frequent revision.

For simple systems, a separate project plan will not usually be required. For medium to complex systems, a project plan may be an important tool for keeping implementations on track. The need for a plan in these cases may be justified by the fact that new software or a new configuration of a highly flexible system is being undertaken, which affects a large number of users or requires extensive resource planning and management.

4.2.2 Specification, Configuration, and Coding

The role of specifications is to enable systems to be developed, verified, and maintained. The number and level of detail of the specifications will vary depending upon the type of system and its intended use. For example, software design specifications are not expected from the regulated organization for non-configured products.

Specifications may be available from the supplier. Before use, the regulated organization should ensure that they are adequate to support subsequent activities, including risk assessment, further specification and development of the system, and verification as appropriate.

For further guidance on specification, configuration, and coding, see Appendix D2 and Appendix D3 of GAMP® 5 [1].

4.2.2.1 Requirements Specification

The extent and detail of requirements should be commensurate with risk, complexity, and novelty, and should be sufficient to support subsequent verification of the system. User Requirements Specifications (URS) should be produced for all laboratory computerized systems. Requirements may not be static, and it may be necessary to review them on an on-going basis, especially if the intended use or regulatory requirements change.

For simple systems or for multiple installations of the same type of system, generic requirements documents may be created. In this way, simple systems can be put quickly into use following their inclusion on any relevant inventories, and maintenance and support plans.

The results of any existing studies, such as business needs analysis, may assist with determining the required extent and detail of requirements definition. It is beneficial to focus on requirements specification and risk assessment early in the project phase as these may drive subsequent verification activities.

The requirements should include both the hardware and software functions. In addition, requirements should include any specific technical or procedural controls that may be required.

The URS should describe what the system should do, based on the intended use of the system and is generally stated in a manner independent of hardware and software, unless a constraint is placed on the system by external factors. For some simple systems, however, it may not be necessary to develop technology-independent requirements due to the limited number of suppliers and the commercial nature of the products.

The supplier-provided list of functions within product information may be used as the basis for defining system functionality. Functions intended to be used and tested, and those functions that are specifically not intended to be used should be identified. Functions not intended to be used are not typically tested, unless indicated by an assessment of risk and potential impact of inadvertent use. If the system does not provide the capability to inactivate undesired functions, procedural controls should be instituted.

Requirements should define the intended limits of operation for the equipment as used in the laboratory. For example, an HPLC pump capable of delivering fluids between 0 mL/min to 20 mL/min may never need to be used at the upper range, if the need is 1 to 5 mL/min. Verifying the pump at the maximum claimed capability may result in rejection of a pump that fully satisfies the intended use.

Systems with greater technical complexity will have greater available functionality and the requirements documents will reflect this complexity. For example, systems with data storage capabilities will have requirements for data handling, data storage, data security, data backup, and possibly electronic records. The team developing the requirements may include:

- SMEs from user area(s)
- Developer(s)
- Quality control and quality assurance or validation representative
- Supplier
- Project manager

One person may fill more than one role for simple systems.

Requirements should:

- Be defined in a way that is unambiguous and explicitly testable or verifiable
- Be prioritized with emphasis on identifying the mandatory requirement

Requirements documentation should reflect the current system. After system acceptance, operational change management should be applied.

Many simple systems, such as air samplers, pH meters, and electronic pipettes are likely to be moved during their lifetime. The need for portability should be identified as a requirement of the system. Laboratory computerized systems which are likely to be moved should be constructed for this purpose. The installation documentation should address risks of movement without adding any undue burden. This aspect also should be considered when planning installation verification. Portability is predicated on the ability to leverage building utilities. If building utilities have not been qualified, potential effects of fluctuating utilities, which may negatively affect the system's performance, should be considered.

For further guidance on the production of URSs, see Appendix D1 of GAMP® 5 [1].

4.2.3 Verification

4.2.3.1 Test Strategy and Testing

Testing demonstrates compliance and fitness for intended use. The test strategy for a laboratory computerized system verifies that a system meets its requirements and is stable, accurate, and precise.

Verification should provide documented evidence of appropriate testing commensurate to the risk to data integrity.

Testing typically covers:

- Installation of hardware, software, and infrastructure
- Functional demonstrations of fitness for intended use and acceptance of the system against requirements
- Additional tests as a result of risk and supplier assessments

The nature of the testing and the level of required stress testing, negative testing, and testing of error handling should be based on risk, complexity, and the results of supplier or product assessment.

In some cases, suppliers of systems may be able to provide testing plans, specifications, and protocols and execute testing. Supplier testing can be useful and may offer time and resource savings. The regulated organization should ensure that supplier testing activities and documentation are adequate to meet their needs.

Verification should provide documented evidence that the system is installed in accordance with engineering and supplier specifications in the production environment and in the test environment if relevant.

This may be based upon the components list described in the purchase order or delivery note (including the make and model numbers for all components) and information supplied by the supplier. Activities may include:

- Identification of components (e.g., hardware: computer, printer, analytical instrument firmware, interfaces, and networks, and documentation) received and undamaged
- Identification of software applications and operating systems
- Verification of environment specifications (if applicable)
- Verification of safety specifications (if applicable)

Functional testing provides documented verification that the system will function according to specifications throughout the anticipated operational range. For purchased systems, functional testing may be based upon the specifications from the supplier.

For some simple systems, such as pH meters, balances, stirrers, water baths, and thermometers, calibration may be an important element of verification. Consistent performance of some common laboratory computerized systems may be demonstrated by a combination of routine system suitability checks, preventive maintenance, and calibration checks, performed according to established procedures. For simple systems, it may be efficient to create generic tests.

For medium systems, the correct operation of the system hardware, software, and firmware should be verified. For these systems, functional testing may be combined with requirements testing.

Requirement testing provides evidence that the system reliably meets requirements in the production environment. This also may be referred to as user acceptance testing or system level testing. Tests should address the procedures that will be used in system operation, including security and data integrity controls.

If a laboratory computerized system is used with identical configuration (computer hardware, operating system, application software, product, and versions) under the same operational and environmental conditions in the same manner across an organization, functional testing may be performed once and referenced by additional installations. Re-execution of some functional tests may be required for subsequent installations and after a system upgrade, operating system upgrade, or major repairs to the system.

For further information, see Appendix 11. See Appendix D5 of GAMP® 5 [1] and the ISPE GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems [13] for a more complete discussion of testing activities.

4.2.4 Reporting and Release

The system should be accepted for use in the operating environment and released into that environment in accordance with a controlled and documented process. Acceptance and release of the system for use for GxP regulated activities should require the approval of the process owner, system owner, and may require approval of quality control or quality assurance.

A computerized system validation report, or equivalent, should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and providing a statement of fitness for intended use of the system. For simple laboratory computerized systems, this may be accomplished through the use of a completed and approved template form.

Deviations or exceptions may include unresolved test failures, requirements not met by the systems, or deviation from planned activities. A risk assessment or impact analysis should be performed on such deviations. Some may be resolved by improving or modifying procedures.

Prior to release of any system into production use, all necessary procedures should be established to assure the continued compliant performance of the system. These may include:

- System listed on inventory
- Appointment of system owner
- Training
- System use log
- System access list
- System maintenance and calibration requirements and procedures
- System SOPs

A release memo or similar, may be generated for complex laboratory computerized systems following (or concurrent with) the approval of the validation report, officially authorizing the use of the system.

For further guidance on validation reporting, see Appendix M7 of GAMP® 5 [1].

4.2.5 Supporting Processes

4.2.5.1 Traceability

Traceability is a process for ensuring that:

- Requirements are addressed and traceable to the appropriate functional and design elements in the specifications.
- Requirements can be traced to the appropriate verification.

As well as demonstrating coverage of design and verification, traceability can assist the assessment and management of change.

Traceability should be focused on aspects critical to patient safety, product quality, and data integrity.

Traceability also can provide benefit in identifying scope of regression testing for changes, and enabling fast and accurate responses during an inspection or audit.

The rigor of traceability should be based on risk, complexity, and novelty. For example, a simple, non-configured system may require traceability only between GxP requirements and their verification.

Traceability may be achieved in a number of ways, including using a Requirements Traceability Matrix (RTM), automated software tools, spreadsheets, or embedding references directly within documents. An RTM may be generated as a separate deliverable or as part of an existing deliverable, such as the requirements document.

Traceability for simple systems can be achieved through common or consistent numbering of requirements, designs, and testing documentation, rather than a separate matrix.

Requirements not met by the system should reference the means by which it is fulfilled, such as a procedural control reference. Unmet requirements that represent functionality requested for future upgrades also may be captured.

The traceability process should be started in parallel with the URS and should be maintained throughout the life cycle of the system. For simple systems with only a few requirements, it may be possible to define user requirements and demonstrate traceability in a single document. For some requirements, it may be valuable to reference the supplier supplied information (e.g., for details such as range of operation).

4.2.5.2 Design Review

Design reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. They are planned and systematic reviews of specifications, design, and development performed at appropriate points throughout the life cycle of the system.

Design review should be performed by appropriate SMEs. The individuals performing the review should be identified. The rigor of the design review process and the extent of documentation should be based on risk, complexity, and novelty.

Detailed design reviews are not typically performed for off-the-shelf non-configured systems. In such cases, the regulated organization usually compares system capabilities with intended use (requirements). By comparing requirements against capabilities, potential gaps can be identified and addressed. There may be cases where gaps cannot be mitigated and an alternative product supplier will need to be selected.

In such cases, additional columns may be added in a traceability matrix. For example:

Table 4.2: Example Traceability Matrix

Requirement	Vendor Reference	Meets Need?	Test Reference
Must weigh from 0.1 to 100 grams	"Can weigh samples from 0.1 to 200 grams (pg. 35)"	Yes	Installation Qualification Test #2: Calibration

4.2.5.3 Change and Configuration Management

Appropriate configuration management processes should be established such that a computerized system and all its constituent components can be identified and defined at any point.

Change management procedures also should be established. The point at which change management is introduced should be defined. Appropriate change processes should be applied to both project and operational phases.

Change management should be applied to each controlled item upon its first formal approval to avoid unintentional or unauthorized change. Different controlled items may require different levels of formality and rigor. The project change management approach should be documented. The project manager and the user should agree the level of user involvement. Project change management processes typically are simpler than those for operational GxP systems, due to fewer personnel involved, faster communication, and lower risk.

4.3 Operation

As part of preparing for final acceptance and formal handover for live operation, the regulated organization should ensure that appropriate operational processes, procedures, and plans have been implemented, and are supported by appropriate training. These procedures and plans may involve the supplier in support and maintenance activities.

Once the system has been accepted and released for use, there is a need to maintain compliance and fitness for intended use throughout its operational life. This is achieved by the use of up to date documented procedures and training that cover use, maintenance, and management.

The operational phase of a system may last many years, and may include changes to software, hardware, the business process, and regulatory requirements. The integrity of the system and its data should be maintained at all times and verified as part of periodic review.

Operational procedures define activities necessary to maintain the system in a compliant state and fit for intended use; these include:

- Calibration
- Problem management
- Change and configuration management
- Maintenance
- Performance monitoring
- Business continuity
- Disaster recovery
- Access control
- System administration
- Backup and archive
- Training
- Periodic review

For many laboratory computerized systems, these procedures are not system specific. Controls should be established so they may be leveraged across systems where possible. Some may be applicable to a class or group of systems rather than individual systems.

There is considerable opportunity for reuse of documents, processes, and procedures during the operation phase for laboratory computerized systems, especially for multiple identical or similar models of equipment. Companies should develop a cost effective, risk-based approach to compliance and fitness for intended use for such systems based upon reuse of documentation. This may be accomplished by creating a master set of documents and templates or forms that can be completed for each new system.

4.3.1 System Hardware Maintenance

Most laboratory computerized systems will require some maintenance throughout its life cycle. Maintenance may be planned, preventive, or corrective. Maintenance and calibration procedures and services may be performed by suppliers if agreed and approved by the regulated organization. Proper maintenance reduces the risk of failure and assures performance, data integrity, and availability.

A record should be kept for all maintenance work. Corrective emergency maintenance also may result in a problem report. For a multi-component system, maintenance records for each component may be required. At a minimum, the work performed, the date, and the person(s) performing the maintenance should be recorded.

Maintenance should be executed in a manner that minimizes potential impact and down time for users. As with problem reporting, any potential changes (including emergencies) should be managed and implemented through the change management process.

In addition to a maintenance record, a use record may be established, containing the date, identity of the user, and actions performed. This may be a notebook located next to a stand-alone instrument, or an electronic application.

For larger systems, a networked data acquisition use record may be implemented electronically, as part of user authentication. One benefit of such a log is the ability to assess the impact on data integrity, when emergent issues are discovered. As such, the information contained in the use records can provide direct input into the problem reporting and change management process.

Any maintenance activities performed by the users of the system also should be documented. When a system requires maintenance that cannot be performed when the system is in routine use, this should be planned to align with scheduling requirements. If the planned maintenance event is missed, any potential impact on the status of the system should be communicated and understood by the end users and maintenance technician.

During maintenance, replaced components or parts should be documented so that the organization can understand the potential impact. Before the system can be returned to service, the correct performance of the system should be confirmed and documented. The same principles also apply when corrective maintenance is performed on a system.

4.3.2 Incident Management

The incident management process aims to categorize incidents to direct them to the most appropriate resource or complementary process to achieve a timely resolution. There should be a procedure defining how problems related to software, hardware, and procedures should be captured, reviewed, prioritized, progressed, escalated, and closed. This includes the need for processes to monitor progress and provide feedback.

Incident reports can provide evidence of necessary changes, which may be fed into the change management process. When a problem is experienced with a laboratory computerized system in one part of an organization, consideration should be given to reporting the event to other users of the system or data generated from the system within the organization.

Additionally, the supplier should have a mechanism for notifying users if a major problem is identified that may have an impact on the reliability and accuracy of the generated results. Incident reports should be reviewed along with the change records, as part of the periodic review program.

Incident management procedures should include documentation updates and timely follow-up of all events, including system failures or malfunctions. Incident reports should include the following:

- Description of the event
- Date and time of occurrence
- Person discovering the event
- Potential impact on operations or data
- Postulated causes, if known
- Suggested corrective actions, based on supplier and user input

All incidents may not result in changes to the system, and some incidents may not be reproducible, but all should be recorded. Typical outcomes include the implementation of:

- Emergency changes (system repairs)
- Procedural changes
- Planned future changes (e.g., new software version)

4.3.3 Corrective and Preventive Action

Corrective and Preventive Action (CAPA) is a process for investigating, understanding, and correcting discrepancies based on root-cause analysis, while attempting to prevent their recurrence. In the operational environment, the CAPA process for computerized systems should feed into or be part of the overall CAPA system used for the rest of operations.

When incidents occur or when opportunities to reduce process/system failures are identified by other means, corrective actions and preventive actions should be identified and processes established to ensure that these are implemented effectively.

4.3.4 Change Management

All changes that are proposed during the operational phase of a computerized system, whether related to software, hardware, infrastructure, or use of the system, should be subject to a formal change management process. This process should ensure that proposed changes are appropriately reviewed to assess impact and risk of implementing the change. The process should ensure that changes are suitably evaluated, authorized, documented, tested, and approved before implementation, and subsequently closed.

All changes – major, minor, cosmetic, or replacing seemingly identical components – can affect the computerized system and possibly introduce unplanned, undesired impact on GxP processes.

The change management process should allow the rigor of the approach, including the extent of documentation and verification, to be scaled based on the nature, risk, and complexity of the change. Some activities such as replacements and routine system administration tasks should be covered by appropriate repair or system administration processes.

The authority and responsibility for review, approval, and implementation of the changes should clearly be defined. The point of transfer from project to operational change management should be clearly defined and documented, e.g., in the computerized system validation plan, validation report, system release documentation, or other means.

Care should be taken when exchanging like-for-like equipment components to ensure that the elements are truly functionally identical.

The change process should address the following key steps:

- Describe the proposed change
- Document and justify the change
- Evaluate risk and complexity of the change
- Define the extent of testing according to risk
- Determine the appropriate approval level
- Communicate the change to stakeholders

- Accept or reject the request for change
- Develop and verify the change
- Approve and implement the change
- Verify implementation
- Close the change

Implementation of emergency changes should be based on risk and should be subsequently reviewed, documented, verified, and approved in a timely fashion according to the appropriate procedure. What constitutes an emergency change should be clearly defined. Changes should not be allowed to escalate to emergency status through the accumulation of internal failures or delays.

While individual changes and their impact are assessed, it is also important to assess the impact of accumulated changes over a time period. This is part of the periodic review, as described in Section 4.3.5 of this Guide.

4.3.5 **Periodic Review**

Periodic reviews are used throughout the operational life of a computerized system to verify that it remains compliant with regulatory requirements, fit for intended use, and satisfies organization policies and procedures. The review should confirm that, for all components of a system, the required support and maintenance processes are established and that the expected regulatory controls (plans, procedures, and records) are established and in use.

A process for timing and scheduling of reviews should be defined. The review periods for specific systems should be based on system impact, complexity, and novelty. These risk-based decisions should be documented.

Problems found during the review should be documented, along with recommended corrective actions. Consideration also should be given to possible wider implications. Agreed corrective actions should be resolved and approved. These activities should be documented.

For further guidance on periodic reviews, see Appendix O8 of GAMP® 5 [1].

4.3.6 **Continuity Management**

Business continuity planning is a series of related activities and processes concerned with ensuring that an organization is fully prepared to respond effectively in the event of failures and disruptions.

Critical business processes and systems supporting these processes should be identified and the risks to each assessed. Plans should be established and exercised to ensure the timely and effective resumption of these critical business processes and systems.

Patient safety, product quality, and data integrity should not be compromised by system failure or breakdown.

System backup, archival, and disaster recovery are closely related to and impact business continuity planning. The following terms are used in this section:

Business Continuity Planning: the act of planning for the continued operation of the laboratory computerized system, laboratory, or site in the event of failures or disruptions.

Business Continuity Plan (BCP): a document prepared to summarize the organization's business continuity activities. BCPs can address single or multiple systems.

Disaster: the sudden and unanticipated loss of use of one or more systems due to an adverse event which may involve the recovery of any or all of the system components, i.e., hardware, software, or data. A disaster is an event that if unmitigated, will interrupt business processes which the system supports.

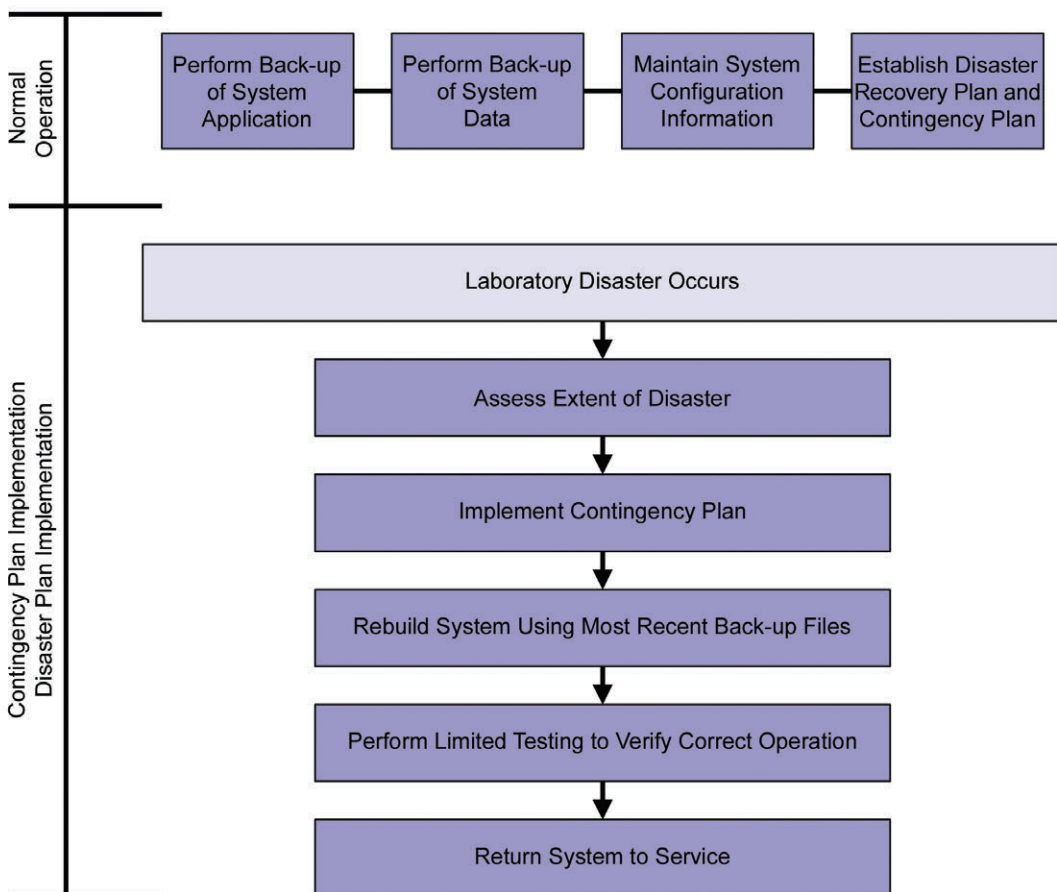
Disaster Recovery: the act of planning for the restoration of systems and facilities after a major incident, e.g., the loss of telecommunications, power, buildings, or major computing facilities. It is essentially a reactive process.

Figure 4.1 shows the interrelated nature of these processes. Activities related to continuity management should be defined according to impact of the instrument on business continuity and the impact of the data generated by the system.

Both the hardware and the software elements of the laboratory computerized system should be considered. Unique systems which have no redundancy in the organization require the most effort and bear the highest risk. For redundant systems, the maintenance of data integrity is one of the most important activities. Where manual processes are invoked to allow the business to continue to operate, it is important to consider how associated electronic records or data will be synchronized once the electronic systems have been restored.

Continuity management activities should be re-assessed periodically. Information from periodic review may help to justify reducing tasks or including additional tasks in the BCPs.

Figure 4.1: Relationship between System Backup, Archival, and Disaster Recovery



Disaster plans, archival, and restoration of backup media should be considered and tested using a risk-based approach during the system project phase.

Simple systems may be easily replaced, can be ordered from multiple suppliers, and are likely to be in operation in several laboratories within a department. Consequently, the plan for continued operation in the face of loss of the system may simply be to use another system or to purchase a new one. If an organization is small or the equipment is unique, a means to continue to operate while the system is being replaced should be considered.

For simple or medium systems, being able to reference documented configurations, such as communication port settings or instrument drivers, (as part of documented configuration) is valuable in recovering or recreating the system or in purchasing a new unit. As a system grows in technical complexity, and data is stored to durable media for the purpose of re-processing, the processes for backup, archive, and restore should be addressed.

For simple and medium systems, the Service Level Agreement (SLA) may govern a group of systems or an entire business unit. For complex systems with higher impact, assistance may be available from the supplier through either a SLA or a maintenance agreement. Depending upon the size of the organization and the complexity of the system, there also may be internal SLAs between the system owner and those responsible for the infrastructure. Further guidance on archive, backup, and disaster recovery is provided in GAMP® 5 [1].

High risk systems without redundancy should be reviewed on an individual basis, as factors such as budgets and available expertise can drive decisions on whether a system should be “recovered” or a replacement unit purchased.

4.3.7 Backup and Restore

Processes and procedures should be established to ensure that backup copies of software, records, and data are made, maintained, and retained for a defined period within safe and secure areas. Restore procedures should be established, tested, and documented.

If the backup process is performed by a supplier (internal or external), the process should be approved by the system owner.

Procedures should be established to cover routine back-up of records, data, and software to a safe storage location, adequately separated from the primary storage location, and at a frequency based on risk. There should be established procedures for recovery following a breakdown to ensure documented restoration and maintenance of GxP records and data.

The back-up procedure, storage facilities, and media selected should ensure an acceptable level of data integrity. There should be a backup log with references to the media used for storage. The media used should be documented and justified for reliability. A Scientific Data Management System (SDMS) may be used to store the data in a central database. The SDMS itself is an IT application which should be controlled and managed according to GAMP® 5 [1].

Backup procedures should consider the verification of the data transfer and the refresh procedures necessary for the media, as well as the environmental specifications and procedures for monitoring the records. Duplicate copies of backup information are usually maintained, locally and remotely, to ensure the information is available should it be needed as a result of a localized disaster. The information should be protected from fire, water, and other hazards.

These processes are all typically the responsibility of the system owner.

For further guidance on backup, see Appendix O9 of GAMP® 5 [1].

4.3.7.1 Security Management

Security management is the process that ensures the confidentiality, integrity, and availability of an organization's regulated systems, records, and processes. Effective security management protects assets to minimize the business impact of security vulnerabilities and incidents.

Measures should be implemented to ensure that GxP regulated computerized systems and data are adequately and securely protected against willful or accidental loss, damage, or unauthorized change.

Such measures should ensure the continuous control, integrity, availability, and (where appropriate) the confidentiality of regulated data.

See Appendix 10, Security Management for Laboratory Computerized Systems.

4.3.8 System Administration

System administrators provide support for the production use of laboratory computerized systems. This includes support for the general computing environment as well as individual systems. The scope of system administration activities will depend on the nature of the system and the organization implementing the system. The established Standard Operating Procedures (SOPs) for system administration should be challenged during testing.

SOPs should describe all necessary functions including control and management of any unique features of the particular system, as well as controls necessary for regulatory compliance. When possible, available system functions should be used to provide the necessary controls. For example, if the intention is to have users change their passwords every 90 days, this setting should be implemented by the computer system so that passwords automatically expire every 90 days. If appropriate system controls, the preferred option, are not available, procedural controls should be developed to supplement the functions of the laboratory computerized system.

To maintain data integrity, the role of the system administrator should be separated from the data analysis generating accounts on the system. System administrators should not perform analysis on the system and should not be involved in the data review and approval process. If this cannot be achieved, it may be possible to mitigate this risk by the creation of two separate accounts, one account for system administration without analysis capabilities and one account for routine analysis without administration rights.

For simple non-networked systems, the boundaries of the laboratory computerized system are easily defined and system administration is frequently performed by a single expert. For complex systems with networked environments, it may be more difficult to define the boundaries of single systems since many systems share the same network infrastructure and system administration tasks may be dispersed among different departments.

For complex systems operating in a network environment, there are typically many applications running in the common computing environment. These systems usually consist of a software application and all supporting software and hardware, personal computers, analytical instruments, interfaces, and servers. In a networked environment; therefore, system administration procedures are likely to be divided into general procedures to support the network environment, plus application specific procedures. Administrative tasks may be divided among specialists in areas such as security, account management, directory services, print, and output management. In this environment, the system administrator of the scientific application would be focused only on the management and support of the application. In a small laboratory network environment, the system administrator may be responsible for providing network services, as well as end user support for the application software.

Decisions should be made as to how system support will be handled, before SOPs are written. This activity should begin during the project phase with input from the concept phase. Such decisions should consider the size, capacities, and capabilities of the computing environment. Large organizations may need to deploy a more sophisticated administrative model with multiple roles and possibly multiple departments defined to perform subsets of administrative functions. Smaller organizations may consolidate functions based upon the amount of work required and the staff available.

Systems not storing data may require only minimal system administration attention. Support may be the administrator contacting the supplier should an issue arise. Even for these simple systems, it is considered best to have a defined system administrator so that there is a single point of control for issues from the laboratory and from the supplier.

Regardless of the size or nature of the organization or system, specific system administration functions should be addressed, such as problem reporting, configuration and change management, and maintenance of user accounts.

Procedures should be established to address how the system administrator will monitor and report suspected security breaches. Procedures also should define the process to monitor and apply security patches and maintain updated virus protection for the system. If an organization policy allows for remote dial-in support of a system or support accounts are installed on the system, the system security procedures should define how access is granted and removed, and how remote user actions are monitored.

4.3.8.1 *Record Management*

Policies for retention of regulated records, including those generated during verification of laboratory computerized systems, should be established, based on a clear understanding of regulatory requirements, and existing corporate policies, standards, and guidelines.

Record retention periods and the locations also should be defined.

Archiving is the process of taking records and data off-line by moving them to a different location or system, usually protecting them against further changes. Procedures for archiving and retrieval of records should be established based on a clear understanding of regulatory requirements.

Archived records should be secured, protected from corruption, damage, loss, and unauthorized changes, and should be retrievable throughout the record retention period required by the applicable regulations, organization policies, and procedures. Over time, archived records may require migration to new formats; the content and meaning of the original record should be maintained.

Where the archiving or migration process is computerized, the robustness of the process and system should be verified to ensure that record content and meaning, and the ability to meet GxP requirements are maintained.

Stored records and data should be initially and then periodically checked for:

- Accessibility
- Durability
- Accuracy
- Completeness

Records and data should be stored under secure, controlled conditions. Determination of the level of required level of control should be risk-based.

Specific requirements, such as the role of the archivist in GLP regulations should be considered and addressed.

For further guidance on archiving, see Appendix O13 of GAMP® 5 [1] and the ISPE GAMP Good Practice Guides: A Risk-Based Approach to Compliant Electronic Records and Signatures [14] and Electronic Data Archiving [15].

4.4 Retirement

This section defines recommended procedures and practices for retirement of laboratory computerized systems including:

- Retirement planning

- Withdrawal
- Decommissioning
- Data migration
- Disposal
- Retirement reporting

Due to the volumes of data and records involved, retirement can be a major task. Consideration should be given to:

- Establishing procedures and controls covering system retirement, including withdrawal, decommissioning, and disposal as appropriate
- Documented evidence to be retained of actions taken during retirement of the system
- GxP records to be maintained, their required retention periods, and which records can be destroyed, including the method of destruction
- The need to migrate records to a new system or archive, and the method of verifying and documenting this process
- The ability to retrieve and use these migrated records on a new system

System retirement may be initiated by various causes. The system may be no longer needed or may be replaced by a different system. This may occur due to a supplier upgrade, the supplier decision to stop supporting the system, or identification of another system better meeting the business needs. Retirement also may be initiated by a catastrophic failure that does not allow the system's continued use.

For systems that do not store data the activities are limited to the archival of any system documentation and the removal of any associated hardware and software. Examples of system documentation may include:

- SOPs
- Manuals
- Specifications
- Installation documentation
- Testing documentation
- Calibration records
- Other documents that may be used to support system verification, operation, and retirement activities such as:
 - Maintenance logs
 - Change management records
 - Periodic review reports

The documentation collected should be indexed and maintained for the required retention period.

For systems that maintain electronic records or data, the focus of the activities is on the integrity and maintenance of these records. This Guide will focus on the retirement of systems that maintain electronic records and data.

Due to the increased use of and reliance on electronic records, along with the fast pace of technology changes and system obsolescence, system retirement activities should be carefully evaluated, planned, and controlled. Procedures and controls should be implemented during the retirement phase of a laboratory computerized system to provide a high degree of assurance that the content and meaning of GxP electronic records are retained for the defined record retention period.

The responsible functional area (e.g., system/business owner, quality control, and quality assurance), should establish a process defining how records will be retained and retrieved during the required record retention period. The process can be documented in the applicable organization policies and procedures and system documentation such as a retirement plan. System stakeholders and their required input into the retirement plan should be defined.

4.4.1 Retirement Planning and Reporting

A system retirement plan describes the documentation and controls, including verification activities, needed to retain and retrieve electronic records in compliance with any applicable regulations. The organization should have documented procedures for the decommissioning or retirement of a system.

Retirement planning and related activities are typically completed when it is determined that a GxP laboratory computerized system will no longer be used for GxP related purposes. However, processes and controls implemented during earlier phases also may impact the scope of system retirement activities. For example, a well-defined and verified process to assure that electronic records generated by the system have been backed-up and archived during the life of system operation may impact retirement activities. Procedures and controls verifying that backed-up or archived records can be restored also may impact the activities that occur during system retirement.

System retirement planning should be completed prior to the system being retired or replaced.

A system retirement report should be generated to summarize the results of retirement activities and to provide any requirements that will be needed to monitor and control subsequent retirement activities.

For further guidance on system retirement, see Appendix M10 of GAMP® 5 [1].

4.4.2 Data Migration

Data migration may be required when:

- An existing system is replaced by a new system
- An operational system experiences a significant change
- The scope of use of a system changes

The migration process should be accurate, complete, and verified.

Mechanisms that may be used to ensure data accuracy and integrity are preserved through the migration process include:

- Sampling data from the entire data set and performing record counts before and after migration
- Printing out a data set (or data sets) before and after migration
- Comparing the data sets to ensure that no changes to the data have taken place

For further guidance on data migration, see Appendix D7 of GAMP® 5 [1].

4.4.3 *Withdrawal, Decommissioning, and Disposal*

Once a retirement plan has been approved and issued, the system should be removed from active operations, i.e., users accounts are deactivated and interfaces disabled. No data should be added to the systems from this point forward. Special access measures may be retained for data reporting, results analysis, and support. Where the system being retired is an analytical instrument (e.g., HPLC) that is configured within a software system (e.g., chromatography data system), the configuration as well as related documentation, should be updated appropriately. Additionally, if there are asset tracking mechanisms which list capital equipment that is undergoing retirement, these should be updated once the system is removed from service.

The controlled shutdown process of a retired system should follow that detailed in the retirement plan.

Data and documentation disposal should be completed using processes in accordance with the defined record retention policy.

As part of instrument disposal, consideration should be given to appropriate decontamination procedures that meet federal regulations and environmental health and safety requirements.

As part of hardware (i.e., server or workstation) disposal, an appropriate organization policy or procedure or defined standard should be applied in order to securely delete sensitive or proprietary information and data, especially to ensure that privacy issues are considered.

For further guidance on disposal, see Appendix M10 of GAMP® 5 [1].

5 Quality Risk Management

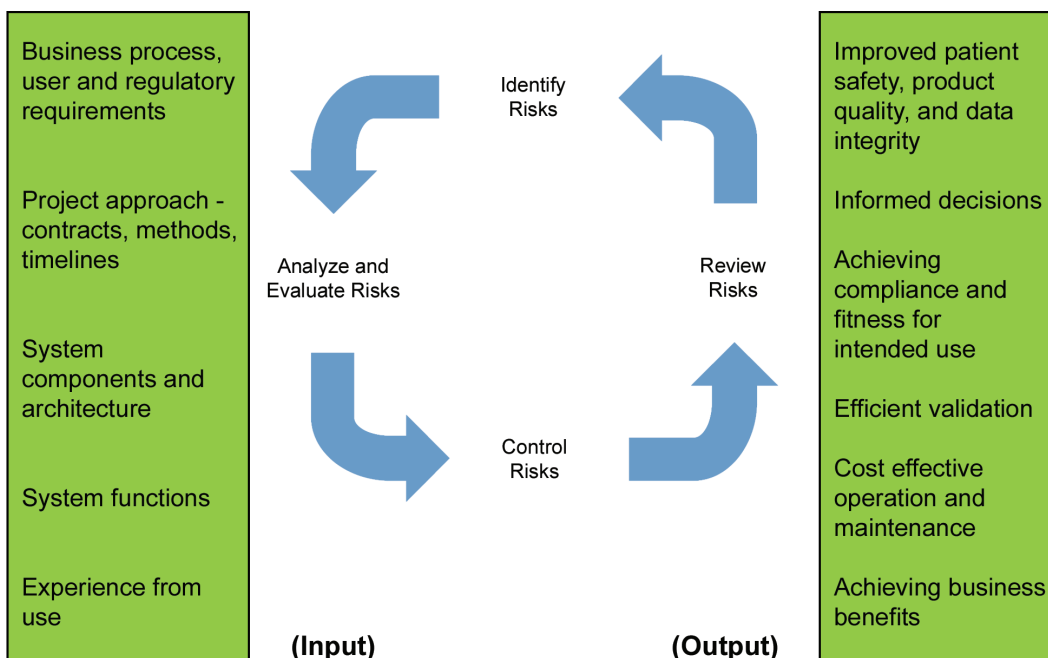
Quality risk management is a systematic process for the assessment, control, mitigation, communication, and review of risks. It is an iterative process used throughout the entire laboratory computerized system life cycle from concept to retirement.

It is used:

- To identify risks and to remove or reduce them to an acceptable level
- As part of a scalable approach that enables regulated companies to select the appropriate life cycle activities for a specific system

Figure 5.1 indicates key areas for risk management and the benefits of the approach.

Figure 5.1: Overview and Benefits of Risk Management



5.1 Science-Based Quality Risk Management

This Guide applies a risk-based approach to the implementation of compliant laboratory computerized systems in a regulated GxP context.

A systematic approach should be defined to verify that the risk associated with laboratory computerized systems has been managed to an acceptable level. The overall extent of verification and the level of detail of documentation should be based on the risk to data integrity, product quality, patient safety, and business continuity, and take into account the complexity and novelty of the system.

The principle product of laboratory computerized systems is testing data which characterizes a product or process. Consequently, the primary risk factor for laboratory computerized systems is assuring that accurate, precise test data is created and retained throughout its life cycle.

5.2 Quality Risk Management Process

This Guide uses the following key terms taken from ICH Q9 [3].

Harm: *damage to health, including the damage that can occur from loss of product quality or availability.*

Hazard: *the potential source of harm.*

Risk: *the combination of the probability of occurrence of harm and the severity of that harm.*

Severity: *a measure of the possible consequences of a hazard.*

Detectability: *likelihood that the fault will be noted before harm occurs.*

Application of quality risk management enables the effort to be focused on critical aspects of laboratory computerized systems in a controlled and justified manner, leading to specific benefits, such as:

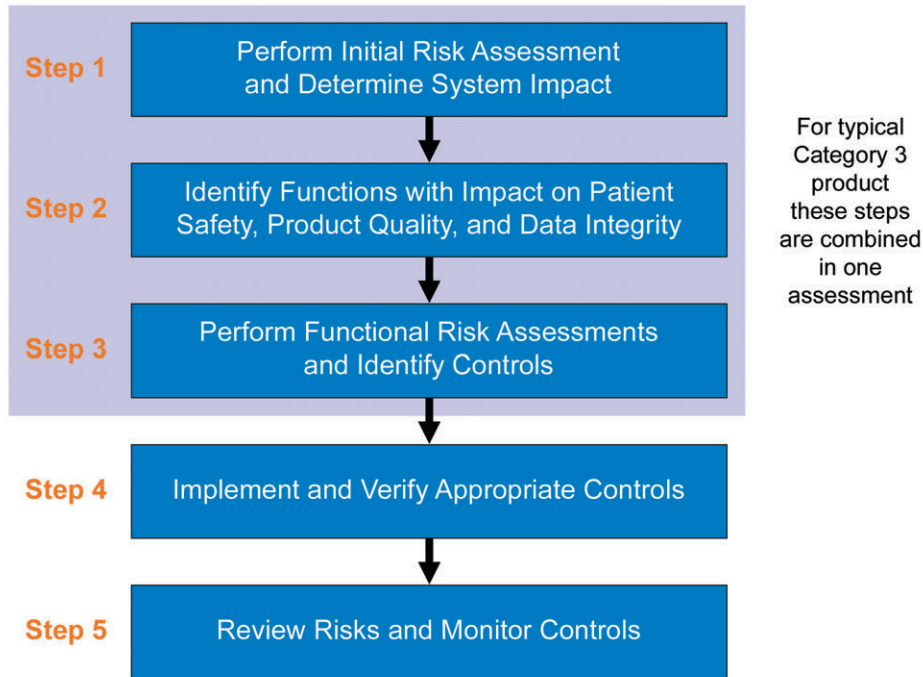
- Identifying and managing risks to data integrity, patient safety, and product quality
- Scaling of life cycle activities and associated documentation according to system impact and risks
- Justifying the use of supplier documentation
- Better understanding of potential risks and proposed controls
- Highlighting of areas where more detailed information is needed
- Improving business process understanding
- Supporting regulatory expectations

5.3 Initial Risk Assessment

Figure 5.2 show the basic steps that may be performed to identify and manage risk for a laboratory computerized system.

For further guidance, see Appendix M3 of GAMP® 5 [1].

Figure 5.2: Quality Risk Management Process Applied to a Laboratory Computerized System

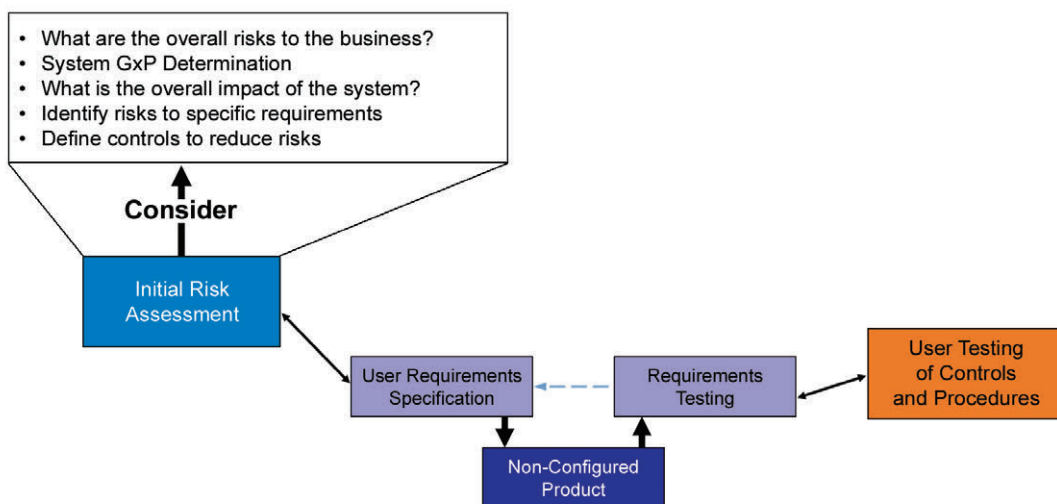


5.3.1 Category 3 Non-Configured Product

For simple systems, the amount of information available at the time of the initial risk assessment may be sufficient for all relevant risks to be identified, assessed, and controlled without the need for further risk assessments.

Figure 5.3 illustrates a risk-based approach for a non-configured product (Category 3).

Figure 5.3: Risk-Based Approach for Non-Configured Product (Category 3)



5.3.2 Category 4 Configured Product

For laboratory computerized systems in Category 4, it may be necessary to carry out additional detailed risk assessments on the specific configuration to support the business process.

Figure 5.4 illustrates a risk-based approach for a configured Product (Category 4).

Figure 5.4: Risk-Based Approach for Configured Product (Category 4)

