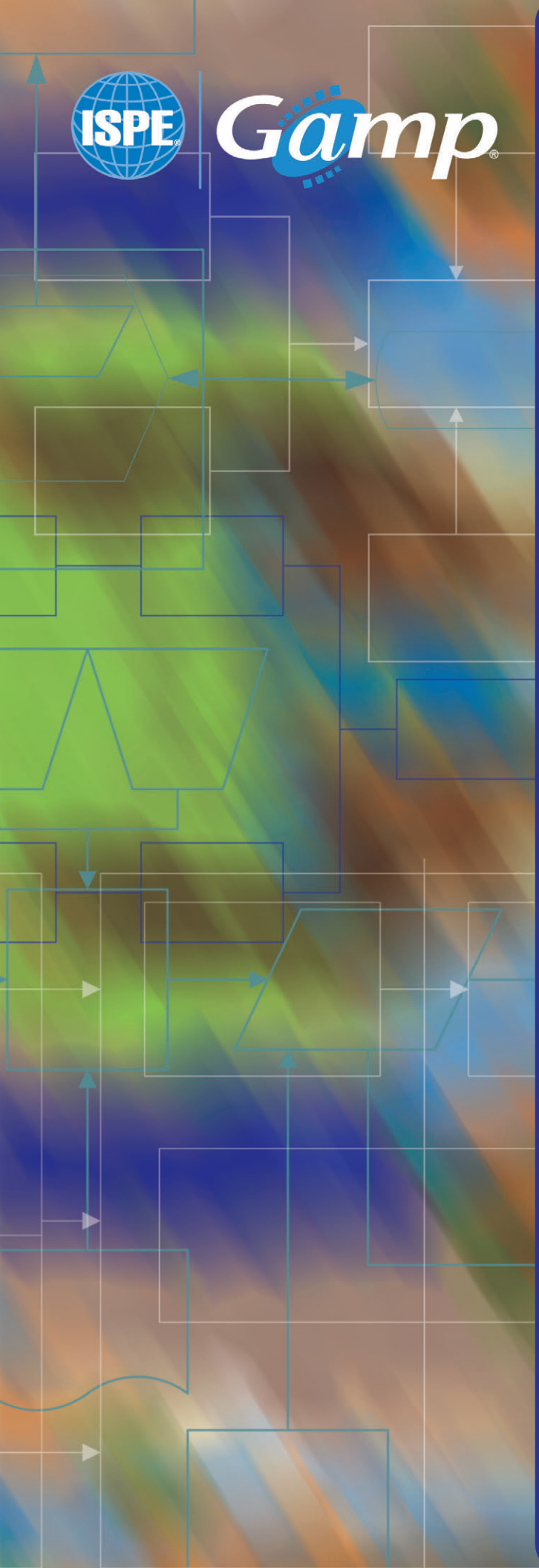


GAMP Good Practice Guide

A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems

Second Edition

What's your approach...

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

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.

SERVICES AVAILABLE

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

"...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.

CQV
An Azzur Group Company

Azzur Group LLC
helping life sciences succeed

Tel: 800.726.0331 Email: info@azzurgroup.com www.azzurgroup.com

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.

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

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
- Appling 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:

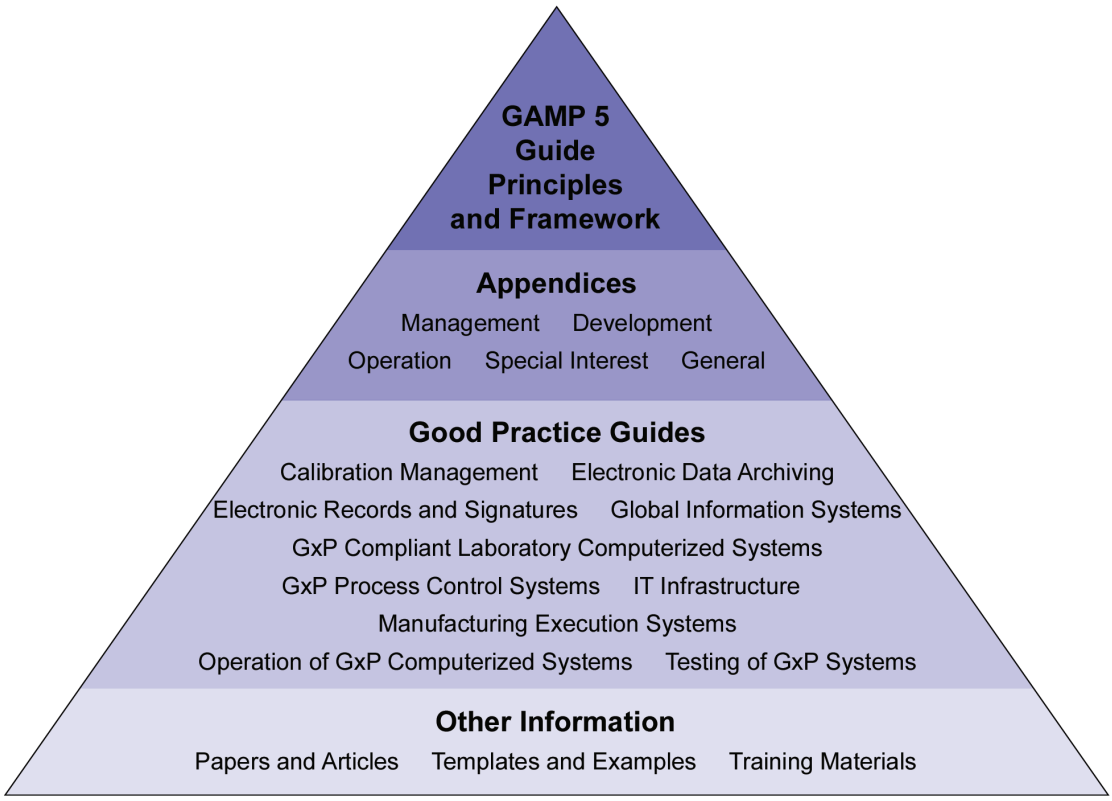
- Reduction of cost and time taken to achieve and maintain compliance
- Early defect identification and resolution leading to reduced impact on cost and schedule
- Cost effective operation and maintenance
- Effective change management and process for continual improvement
- Enabling of innovation and 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 211.160(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

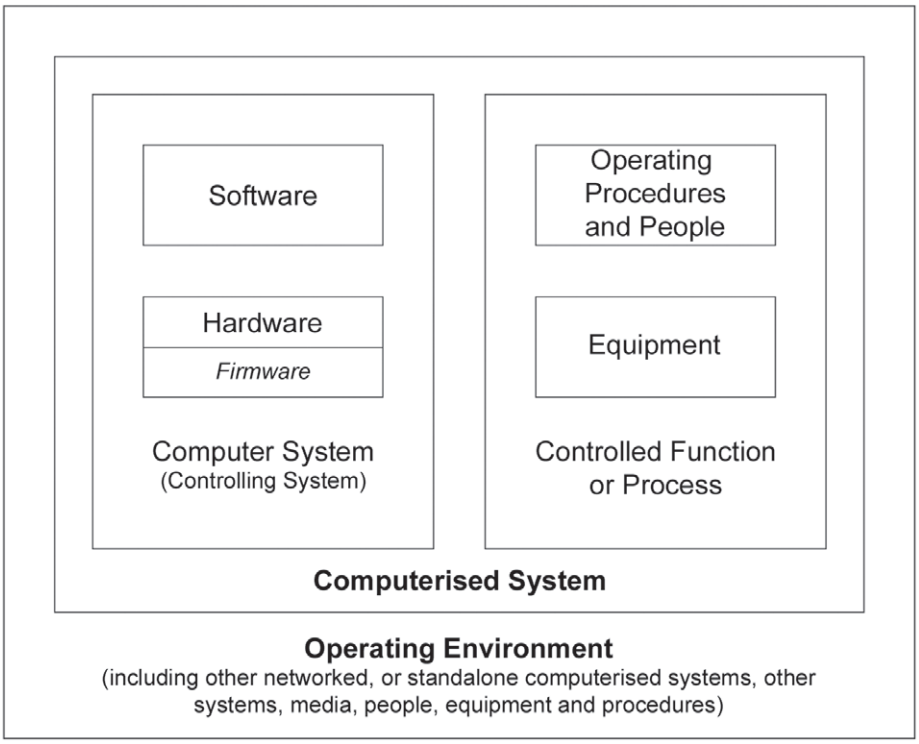
Calibration

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).

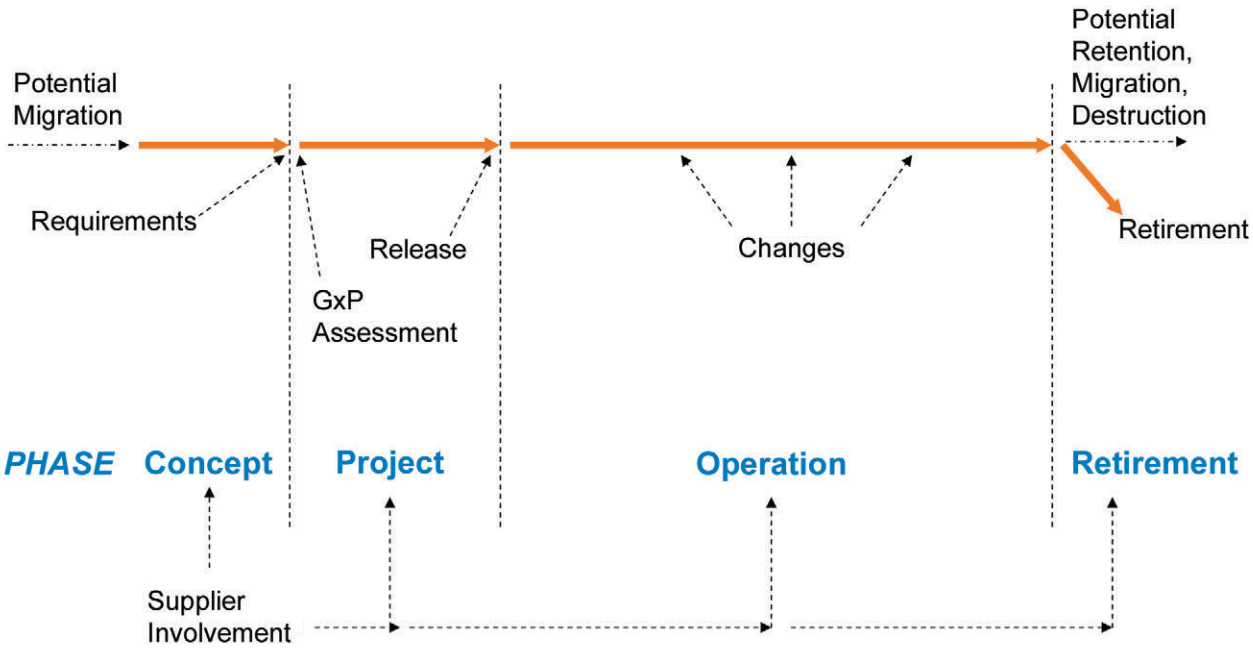
3.1 Computerized System Life Cycle

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

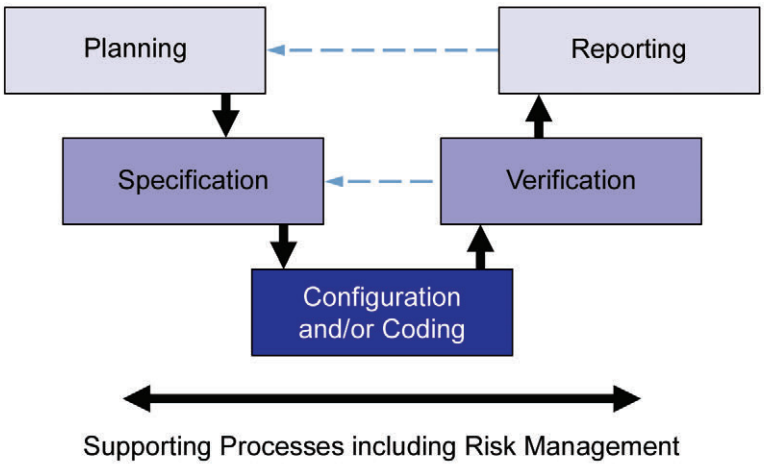


3.2 Specification and Verification

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: • 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.

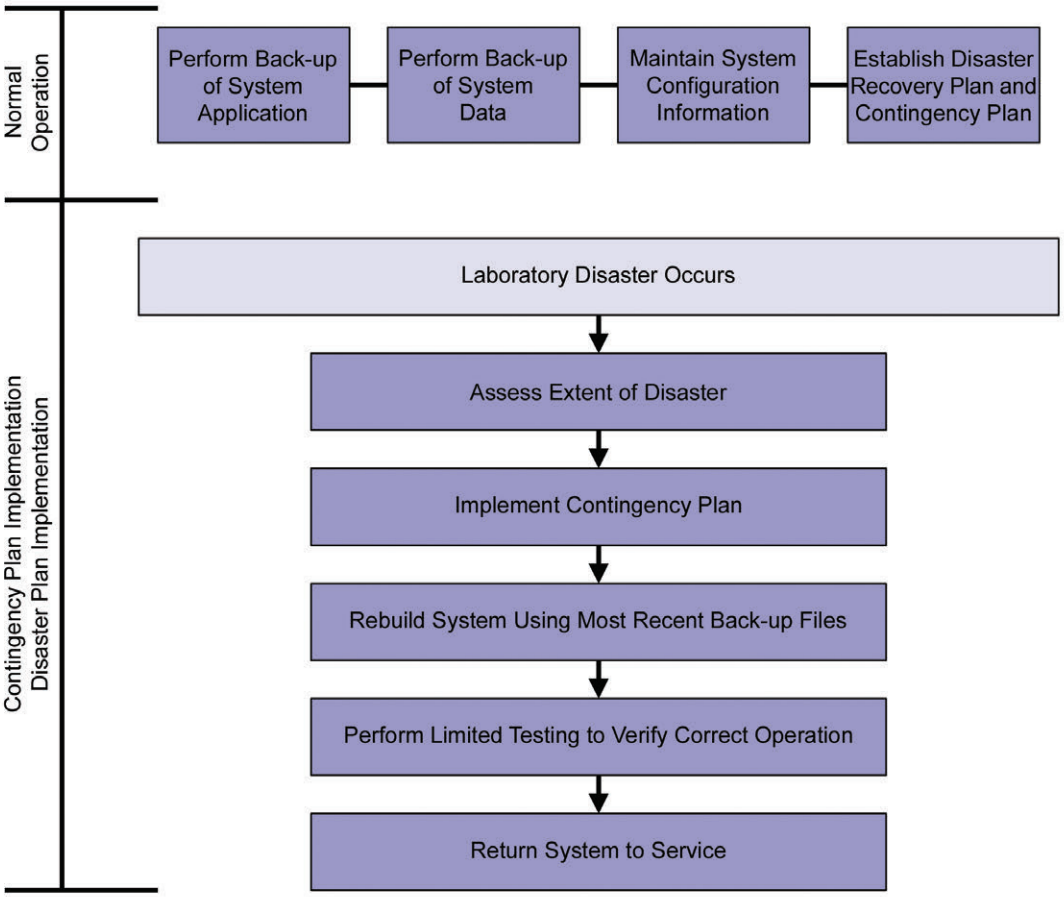
Disaster Recovery: the act of planning for the restoration of systems and facilities after a major incident, e.g., the loss of telecommunications, power, buildings, or major computing facilities. It is essentially a reactive process.

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 to 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

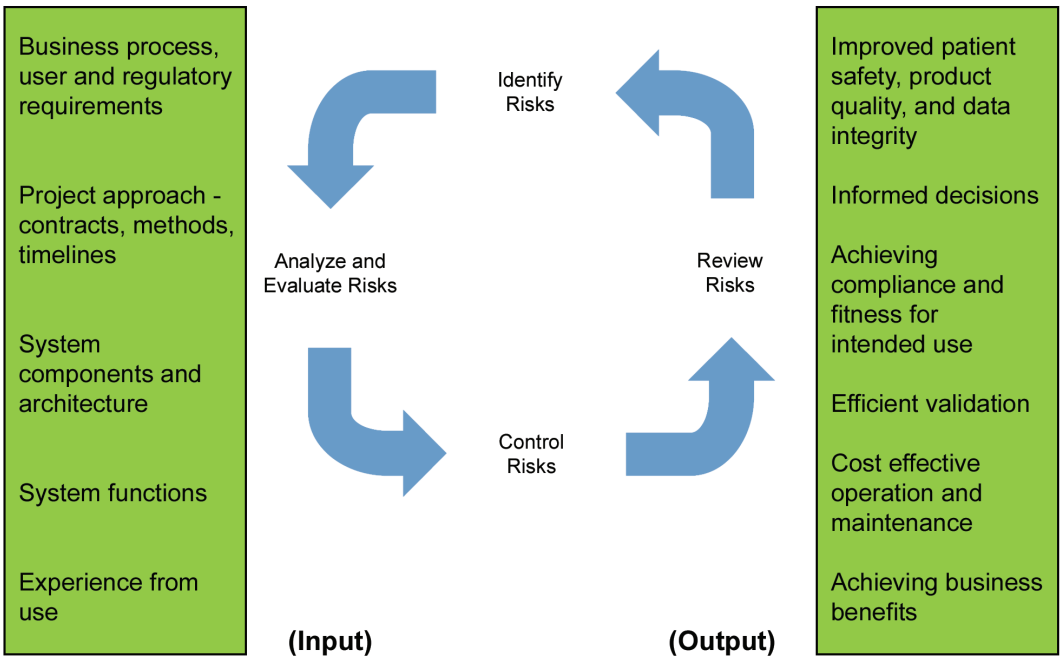
Quality risk management is a systematic process for the assessment, control, mitigation, communication, and review of risks. It is an iterative process used throughout the entire laboratory computerized system life cycle from concept to retirement.

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:

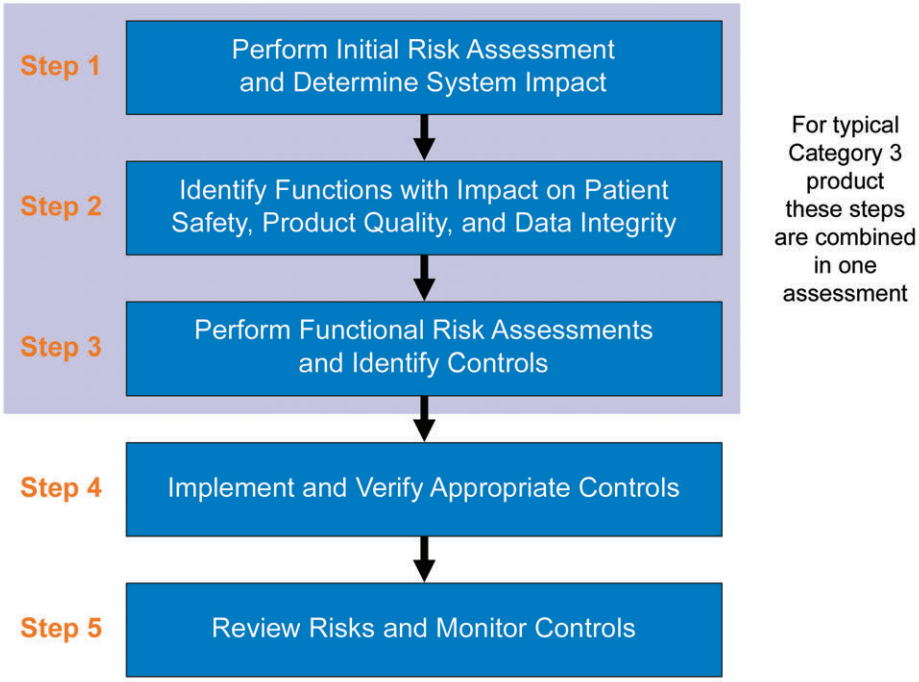
- Identifying and managing risks to data integrity, patient safety, and product quality
- Scaling of life cycle activities and associated documentation according to system impact and risks
- Justifying the use of supplier documentation
- Better understanding of potential risks and proposed controls
- 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

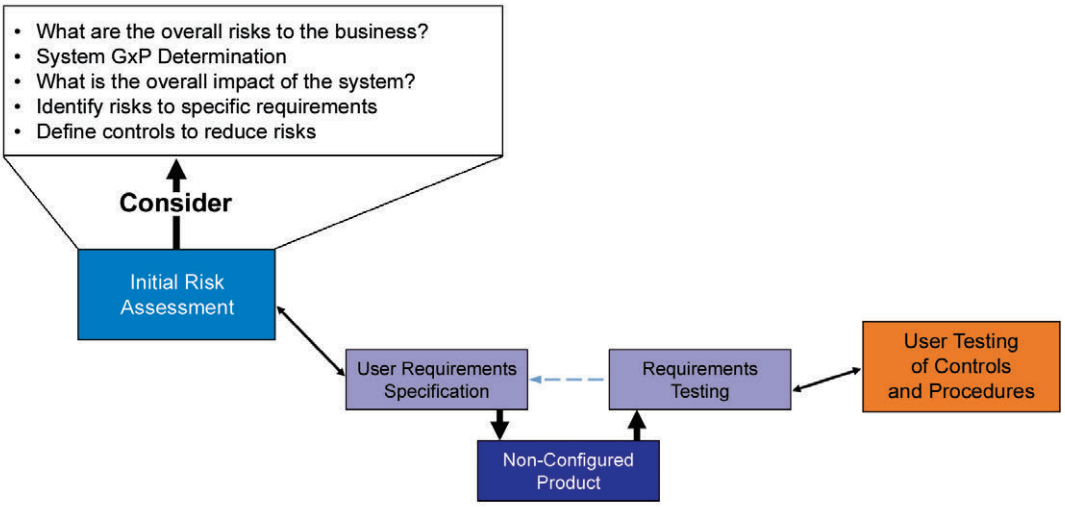


5.3.1 Category 3 Non-Configured Product

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)

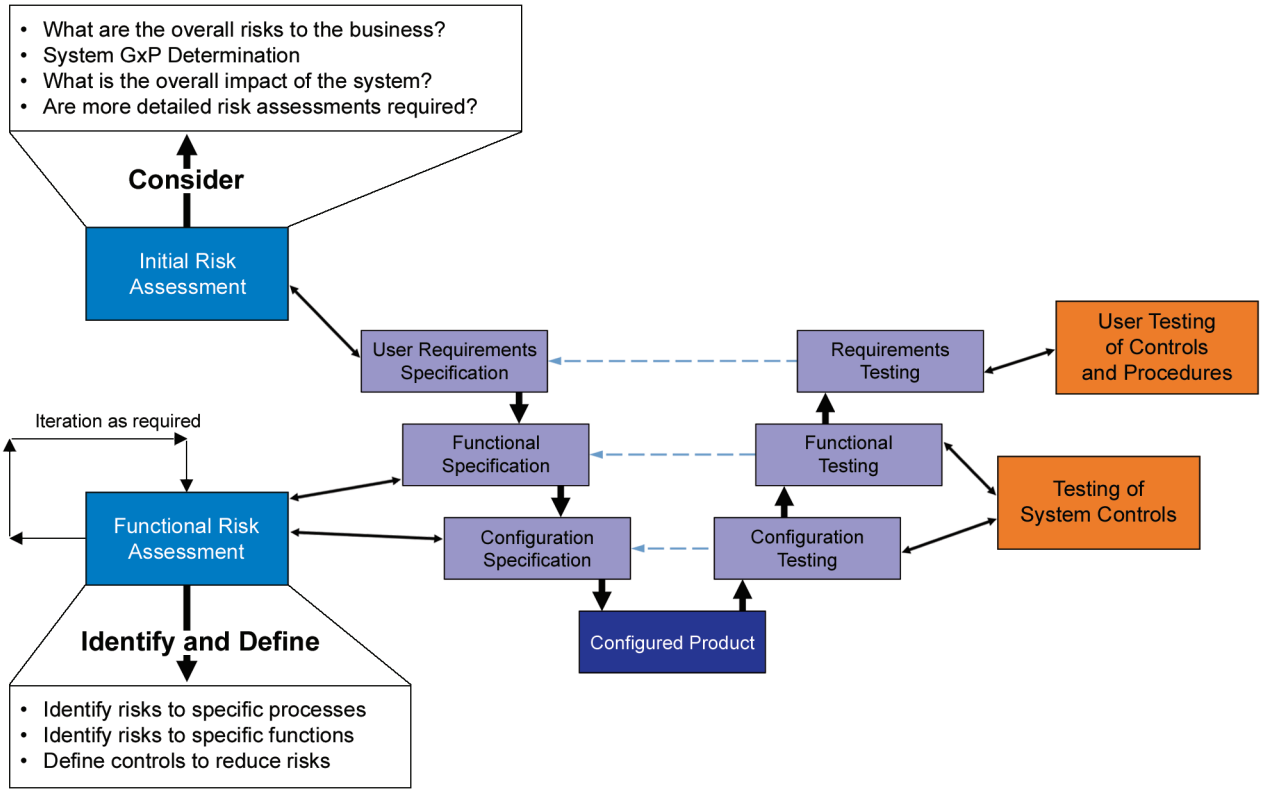


5.3.2 *Category 4 Configured Product*

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).

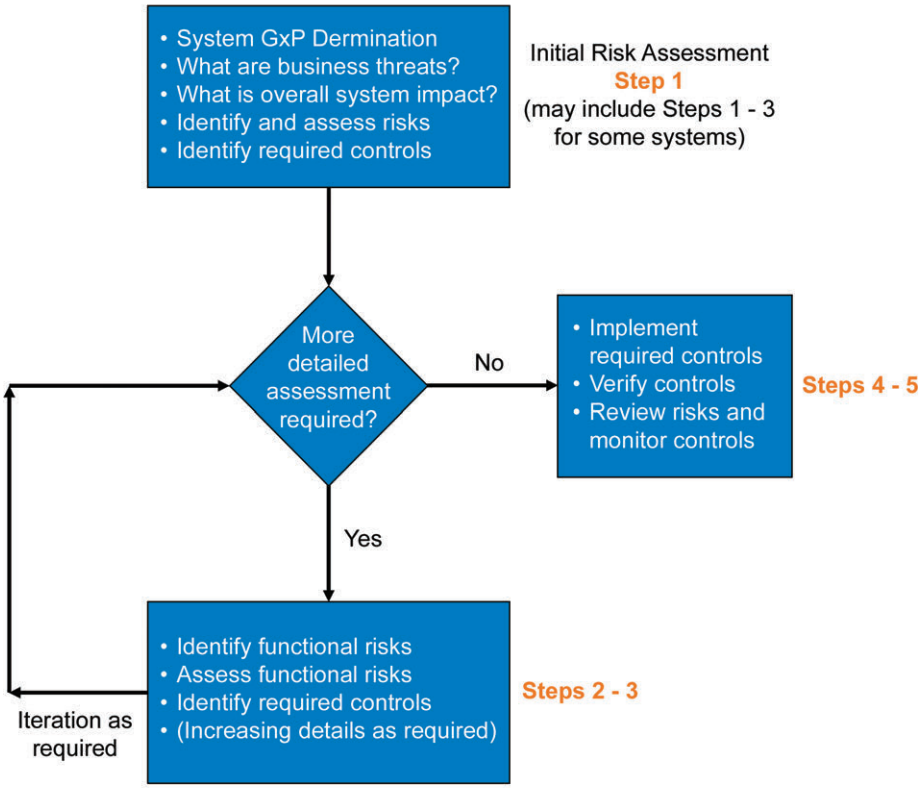
Figure 5.4: Risk-Based Approach for Configured Product (Category 4)



5.3.3 *Deciding the Need for Further Assessment*

Using the steps noted in Figure 5.2, it may be determined that further risk assessments may be needed for the specific configuration and should follow the process noted in Figure 5.5.

Figure 5.5: Deciding on the Need for Further Assessment



5.3.4 *Determining System and Functional Impact*

Depending upon the complexity of the system configuration to support the business process, further analysis may be required.

For further guidance, see Sections 7.2 through 7.5 Appendix M3 of GAMP® 5 [1], which provide examples for analyzing the business process in the five-step process of assessing and evaluating risk.

5.4 Implement and Verify Appropriate Controls

The control measures identified should be implemented and verified to ensure that they have been implemented successfully. Controls should be traceable to the relevant identified risks.

The verification activity should demonstrate that the controls are effective in performing the required risk reduction.

5.5 Review Risks and Monitor Controls

During periodic review of systems or at other defined points, an organization should review the risks. The review should verify that controls are still effective and corrective action should be taken under change management if deficiencies are found.

The organization should consider whether:

- Previously unrecognized hazards are present
- The estimated risk(s) arising from a hazard is no longer acceptable
- The original assessment is otherwise invalidated

If necessary, the results of the evaluation should be fed back as an input to the risk management process, and a review of the appropriate steps of risk management process for the system considered. If there is a potential that the residual risk(s) or its acceptability has changed, the impact on previously implemented risk control measures should be considered, and results of the evaluation documented. The laboratory is responsible for managing risks incurred by suppliers of support services.

6 Regulated Organization Activities

Responsibility for the compliance of laboratory computerized systems lies with the regulated organization, even if development or support services are performed outside the organization. This involves activities at both the organizational level and at the individual systems level.

Therefore, this section is divided into:

- Governance for achieving compliance
- System specific activities

6.1 Governance for Achieving Compliance

Achieving robust, cost effective compliance requires strong governance. Key elements of successful governance include the following:

- Policies and procedures for laboratory computerized systems
- Clear roles and responsibilities
- Training
- Managing supplier relationships
- Maintaining a system inventory
- Quality planning
- Continual improvement activities
- Performing regular essential system maintenance

Effective governance is achieved by integrating these activities into the management of the organization. These activities are described in detail in GAMP® 5 [1], and are not repeated here.

6.1.1 Identify Compliance Standards

Compliance and fitness for intended use should be achieved in accordance with applicable organization policies and procedures. Industry guidance should not supersede organization policies and procedures. The aim should be to achieve compliance and fitness for intended use for all GxP regulated systems in a pragmatic and efficient manner.

6.1.2 Maintaining the System Inventory

Regulated organizations should maintain an inventory of computerized systems, showing which systems are GxP regulated. The inventory should provide summary information such as the:

- Validation status
- Ownership
- Impact

- Current system version
- Supplier

The inventory should be at the level of systems that support business processes, rather than individual items of hardware, which would be covered by local procedures and documentation. Laboratory computerized systems regularly comprise interchangeable instruments, and documentation should be sufficiently detailed to adequately track these individual system components. Configuration logs listing each component of hardware and software, including software versions and documentation can be useful tools in maintaining system compliance.

The system inventory may be used for planning periodic reviews.

6.1.3 Continual Improvement Activities

The regulated organization should conduct periodic evaluation of the policies and procedures used to achieve and maintain compliance to ensure continual process improvement and to ensure that systems continue to be fit for their intended use. It also should verify that the controls, which have been established for the system, are still effective. Continual improvement activities may include communicating changes to service providers and negotiating new service agreements. The organization should consider any new or revised regulations or changes in interpretations.

Understanding the effectiveness of the current processes used to achieve and maintain compliance is best gained by considering current levels of conformance to the process (e.g., established by audit and trending performance) and by reviewing current processes against recognized good practices. The technical, business, and quality groups should all be involved.

6.2 System Specific Activities

6.2.1 Identify System

Although a system description or overview is not necessary for very simple laboratory equipment, they may be required and valuable for more high-risk complex systems. For further information, see Appendix 2.

A system description can serve as a tool to introduce users, such as laboratory scientists, to a system and also can be used to demonstrate process and system understanding to a regulator during inspections.

6.2.2 Identify Key Individuals

Identifying clear roles and responsibilities is critical to a successful implementation in a regulated environment. The key roles are:

- Process Owner – ultimately responsible for ensuring that the computerized system and its operation are in compliance and fit for intended use
- System Owner – responsible for the availability and support and maintenance of a system and for the security of the data residing on that system
- Quality Control and Quality Assurance – clear understanding of the quality and compliance requirements and expectations
- SME
- Supplier

- User(s)
- Support maintenance and calibration staff

These roles are important to ensure the successful understanding and operation of the system throughout its life cycle. Designated individuals should have sufficient experience and training to perform their respective roles. It is acceptable for a single individual to assume multiple roles. When a single individual assumes multiple roles, it is important to ensure that these roles do not represent a conflict of interest (e.g., quality and system owner; they cannot write and review their own documents).

As a single system can be comprised of several units or components and software operating platforms, key roles can become more ambiguous and overlap. Additionally, depending upon the complexity of the system and the implementation, there may be one or more suppliers involved in the project. The role of the supplier is important as the majority of laboratory computerized systems are based on commercially available products. It is the regulated organization's responsibility to ensure the supplier understands all specific requirements for successful implementation of the system.

6.2.3 Training

In order to realize the maximum potential of a system, a properly designed, implemented, and documented training program should be established. Training should evaluate and document competency rather than course attendance. Training, together with education and experience, is the process that ensures those who implement, maintain, or use laboratory computerized systems are able to perform their assigned tasks. SOPs alone are inadequate to guarantee that personnel are competent to perform their assigned tasks. A training program should ensure that the system is being implemented, used, and supported by qualified personnel. Training should be specific to each role. There may be additional roles of individuals who may need specific training identified in the implementation phase including:

- Validation personnel
- Internal auditors
- Document control personnel
- Third party consultants, involved with the project

Programs should be designed and tailored to meet the needs of the individuals and may include:

- Organization policies and SOPs
- Regulatory GxP training
- Validation training
- Safety training
- Software/hardware training
- Laboratory test methods
- Instrument training (including calibration and maintenance)
- Equipment use certification

The process owner is ultimately responsible for ensuring that all relevant persons are adequately trained. This responsibility may be delegated, e.g., maintenance staff may be the responsibility of the system owner and development staff may be the responsibility of the project manager.

A training program should be developed prior to the implementation of a system and reviewed periodically. Training may take the form of:

- Supplier provided training using prepared scripts
- Peer to peer training using prepared scripts
- Expert user to peer training using prepared scripts
- Independent review of procedure with built in tests
- E-learning with built in tests

Both internal and external training sources need to be considered to achieve the proper level of training. Individuals may “self train,” whereby they attest that they have read and understood the procedure. It is important to remember that the qualifications of the trainer also need to be considered and found to be acceptable. Documented proof should be kept up to date in a secure location and reviewed periodically to ensure a proper level of training has been maintained for each individual. Evidence of training should be documented, kept up to date, maintained securely, and reviewed periodically. Documentation also needs to include personnel backgrounds including education, training, and experience.

Training programs and training records demonstrate that the systems are being operated by qualified and trained personnel. Training records and programs should be periodically reviewed for accuracy. As upgrades to laboratory computerized systems occur, there may be a need for refresher training or re-training to ensure that laboratory personnel are trained to the most current methods, functionality, and technology needed to perform their job functions.

A risk-based approach should be used to determine the rigor of training required including measuring effectiveness of training.

7 Supplier Relationships

The relationship between supplier and regulated organization will vary significantly depending upon the product, application, or service being provided, and should be appropriate to the supply and use of the system in a regulated environment. The depth of trust needed between the supplier and the regulated organization is influenced by the complexity and novelty of the laboratory computerized system supplied, and the ability of the user to fully verify the correct functioning of the system.

If the system is a simple purchased off-the-shelf system and does not require configuration to support the regulated organization's business process, or uses the default configuration, supplier involvement is typically limited to supplying the system and documentation. Additional support by the supplier may be provided in the form of installation, verification procedures, training, maintenance, and calibration services. The responsibility for the initial and continued development of the product is the responsibility of the supplier in accordance with good practices.

If the product requires added configuration to support specific business processes, supplier involvement with the regulated organization will typically be increased to include support with specification, configuration, verification, and operation of the system. For example, some system suppliers are able to provide field based specifications for laboratories to use when verifying system performance. Proposed configuration changes by the supplier must be understood by the users. Change notifications should contain information that enables the users to perform any necessary impact analysis prior to acceptance of changes.

As the complexity or novelty of the system increases, there is an increasing need to rely on the work undertaken by the supplier to develop their system. This includes the provision of appropriate documentation, procedures, training, application, and technical support. The greater the complexity, novelty, and/or configuration requirements, the more important it is that both parties have an agreed and clear understanding of the expectations and responsibilities that they are required to satisfy.

The relationship should be based on agreed processes. Procedures to follow should be agreed between the regulated organization and the supplier and be documented in the appropriate plan. Procedures adopted may be those of the regulated organization or from the supplier's quality management system.

The regulated organization should recognize that supplier software is proprietary, and that documentation may not be designed for use by external companies. The confidentiality of the supplier's hardware and software also should be respected.

Service level agreements should be established to define supplier responsibilities related to maintenance and support, including responsibilities during regulatory inspections if necessary. These agreements should include requirements that personnel performing remediation or maintenance operations are adequately trained and that they comply with relevant regulations, as appropriate.

Change management procedures should be established by the regulated organization to ensure that supplier provided firmware or software upgrades are assessed for risk and appropriately tested where necessary. Suppliers also may be employed to provide operating system or network hot fixes or patches. In this case, it is important to maintain adequate communication between all parties involved.

Appendix 11 provides suppliers with guidance on meeting the requirements and expectations of the regulated organization, including the types of documentation and activities required.

7.1 Leveraging Supplier Knowledge and Documentation

Regulated companies may wish to leverage supplier knowledge and documentation, subject to suitability. There may be beneficial to use the supplier documentation as part of the supporting analysis of the system's intended use. For example, the supplier may provide testing specifications that establish the proper installation, functioning, and on-going calibration of the system and these can be leveraged to evaluate system use in the regulated organization's environment.

It is the responsibility of the system owner to evaluate supplier documentation to determine their suitability to support the intended use of the system as a component of the risk-based assessment for the particular application. Factors to be considered in this assessment include:

- Complexity of the system
- Supplier presence in industry (small versus large manufacturer)
- System owner requirements for intended use
- Supplier assessment

Processes that can affect data integrity such as security, audit trails, or calculations should be assessed and supplemented as needed. Supplier documentation may show that the system is functioning according to design, but the system owner has the responsibility to assess and determine whether the system is adequate for its intended use.

7.2 Supplier Assessment

Suppliers should be appropriately assessed, and this may be conducted on-site depending on risk, complexity, and novelty of the laboratory computerized system. The results allow regulated companies to scale their implementation activities. Greater knowledge and trust of supplier practices can result in faster implementation by the regulated organization. For a trusted supplier, less verification may be required; while a supplier whose assessment found deficiencies may require the regulated organization to perform more supervisory activities, especially with high-risk functionality.

A supplier assessment reviews existing standards, processes, and practices. Supplier assessments offer the most value when performed pre-purchase. The documented assessment will compare the supplier's overall quality system against quality expectations of the laboratory. If there are deficiencies in the supplier's system, the assessment will either detail activities to mitigate the issues or the rationale for rejecting the supplier.

The type and depth of a supplier assessment should be based upon:

- The criticality of the system
- The risks to data integrity associated with intended use of the system
- Complexity, e.g., instrument design, data flow, laboratory process
- The ability to verify system functionality within the laboratory

Other factors to consider when determining the extent of supplier assessment include:

- Maturity of the product, e.g., version level of the system/software and length of time on the market

- The history of the use of the system within a regulated industry
- Existing knowledge of the supplier, both in GxP requirements and technical competence.
- Knowledge of the supplier's quality management practices
- The results from and period of time since previous assessments
- Other quality certifications implemented, e.g., ISO 9001 [16]

Supplier assessments complement and may be able to reduce the level of on-site testing required; however, they do not eliminate the need for the regulated organization to conduct testing to demonstrate the system meets regulated organization requirements and is fit for its intended purpose.

Supplier assessments should be part of an on-going process of discovery and improvement that forms the basis for a good supplier-client relationship. Depending upon the criticality and complexity of the system, it may be appropriate to conduct supplier assessments throughout the system development or implementation life cycle and may include system implementers, as well as the supplier if different. Appendix M2 of GAMP® 5 [1] provides detailed information on supplier assessments.

In the laboratory, a single supplier product may operate several key laboratory computerized systems. For example, one operating software platform may be chosen to control the majority of a laboratory's chromatographic instrumentation; in this case, the laboratory needs to critically evaluate the level of risk associated with the supplier. Supplier assessment can assist with understanding and managing these risks.

8 Appendix 1 – Categories of Software

Traditionally, approaches to the qualification or validation of laboratory computerized systems were based upon separating systems into categories. Categorization schemes were mainly based on the hardware components of the systems or on the software complexity of the systems.

The categorization scheme described in the first edition of the ISPE GAMP Good Practice Guide: Validation of Laboratory Computerized Systems was based upon characteristics of systems such as technical complexity, data processing, and data storage abilities. Once a system categorization was determined, the necessary life cycle activities were based upon this categorization.

This Guide presents a continuum of activities based upon risks incurred by the business when operating a laboratory computerized system in their environment for their business process, rather than discreet subcategories. This approach:

- Requires a more detailed knowledge of the use and function of the laboratory computerized system to determine the necessary verification activities
- Is based upon the risk of the individual system, rather than its placement within a category
- Can achieve greater efficiency, by allowing personnel to focus on activities that ensure that data is both valid and trustworthy

Users should understand the factors that would lead to an increase in the amount of a specific life cycle activity.

A thorough understanding and knowledge of a system is needed in order to determine and scale activities appropriately. The complexity and novelty of a system should be understood, along with its impact on:

- Patient safety
- Product quality
- Data integrity
- Business process

The approach described in this edition of the Guide allows the user to focus on activities that address risk and add value to the system. This approach will lead to a focused set of deliverables supporting system use and addressing the risks to data integrity.

Although laboratory scientists may not understand verification activities, they normally do understand which aspects of system operation are important to them, the business process, and the risk to the integrity of data based upon system use.

Laboratory computerized systems are typically purchased systems which are categorized as GAMP® 5 Category 3 and Category 4 systems although there may be some aspects of these systems that would be Category 5, e.g., macros.

Table 8.1 compares the categorizations defined in GAMP Good Practice Guide (GPG): Validation of Laboratory Computerized Systems First Edition (based on GAMP® 4) with those defined in GAMP® 5.

Table 8.1: Comparison of Categories in the First and Second Editions of the Guide

GAMP Good Practice Guide (GPG): Validation of Laboratory Computerized Systems (First Edition)	**GAMP Good Practice Guide (GPG): A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems (Second Edition)**
GAMP Category 1 Out of scope of Good Practice Guide	GAMP® 5 – Category 1 Infrastructure Software Out of scope of this Good Practice Guide
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory A • Software and configuration is not modifiable: • No computer interface used: • Does not produce raw data or test results	GAMP® 5 – Category 3 Non-Configured Products Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process Firmware-based applications COTS software Instruments
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory B • Software and configuration is not modifiable • No computer interface used • Produces raw data or test results, but records not stored or processed	
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory C • Configuration parameters stored and reused • No computer interface used • Process Parameters input and stored • Produces raw data or test results, but records not stored or processed	
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory D • Configuration parameters stored and reused • May have 1 to 1 ratio (computer to instrument interface, server to client interface) • Data manipulated by a separate program external to the system • Process parameters input and stored • Produces raw data or test results which are stored, but not processed	
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory E • Configuration parameters stored and reused • May have 1 to many ratio (computer to instrument interface, server to client interface) • Post-acquisition processing done as part of the system (can analyze data with proprietary data handling system) • Process parameters input and stored • Produces raw data or test results which are stored and processed	

Table 8.1: Comparison of Categories in the First and Second Editions of the Guide (continued)

GAMP Good Practice Guide (GPG): Validation of Laboratory Computerized Systems (First Edition)	**GAMP Good Practice Guide (GPG): A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems (Second Edition)**
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory F • Configuration parameters stored and reused • Proprietary configurable elements • May have 1 to many ratio (computer to instrument interface, server to client interface) • Post-acquisition processing done as part of the system (can analyze data with proprietary data handling system) • Process parameters input and stored • Produces raw data or test results which are stored and processed	GAMP® 5 – Category 4 Configured Products Software, often very complex, that can be configured by the user to meet the specific needs of the user's business process. Software code is not altered: • LIMS • Data acquisition systems • CDS • Spreadsheets Note: specific examples of the above system types may contain substantial custom elements.
GAMP GPG: Validation of Laboratory Computerized Systems (First Edition) – subcategory G • Custom System	GAMP® 5 – Category 5 Out of scope of Good Practice Guide

Two examples, laboratory mechanical pipettes and a sonic bath, are provided to illustrate the logic in moving from discrete categories toward risk-based activities. These examples also illustrate how a classification scheme based only upon the equipment type and followed without consideration of added technical capabilities, could lead to the establishment of inadequate controls.

Example 1: Laboratory Mechanical Pipettes

Traditional mechanical pipettes are hardware devices and outside the scope of this Guide. More complex pipettes, with delivery volumes which are entered electronically, permit users to move solutions with the push of a button, thereby reducing fatigue. These pipettes have firmware control, generate no data, and are typically calibrated manually. These pipettes are simple laboratory computerized systems. Calibration is usually the only test activity performed. Some failures for these pipettes are immediately detectable (e.g., visible solution creep or dripping), other failures are detected only through periodic calibration, performed at risk-based intervals (e.g., how many days of testing are you willing to put at risk?).

More complex pipettes allow users to program the delivery volume and the rate of fluid movement to permit use across a wide range of solution viscosities. These pipettes are firmware controlled and store configuration settings. The configuration record should be protected from unplanned modification, documented, and reviewed at appropriate intervals because pipette performance has a direct impact on the test result. Without review to mitigate the risk of unplanned configuration changes, such modifications could go undetected for long periods. In addition, these pipettes are subject to risks from drifting out of calibration; as are the simpler pipettes. In addition, these pipettes require security and configuration testing, and rely on the supplier's quality system; it is considered impracticable for users to test every possible configuration setting. These are medium complexity systems that require special attention to configuration management to assure test result integrity.

The scenarios described in this example show how added technical capabilities require additional risk-based activities, and how a classification scheme, based on equipment type alone, can mislead users into a false sense of control.

Example 2: Sonic Bath

In the first scenario a standard sonic bath is used simply to dissolve material in volumetric flasks and observation is used to determine if the material has dissolved. If this system can be classified as a computer system, it could be classified as (a simple) GAMP® 5 Category 3. Conformance with requirements can be easily verified and documented by observation of operation. In this case, the requirements and the verification activities for the system are very basic.

However, if the use of the sonic bath requires that a specific amount of sonic energy be used, this scenario adds a level of complexity to the requirements for this sonic bath. Though classified as a GAMP® 5 Category 3, this added complexity of the requirements adds risk which necessitates additional verification activities. In this example, there is a need to document procedures for the calibration of the sonic energy levels of the bath.

Building upon the system complexity, consider the risk associated with this sonic bath integrated and used within a robotic system. In this scenario, the robotic system would be a GAMP® 5 Category 4 configured system. Verification activities for the bath as a standalone system and verification activities necessary for the integration of this system within the robotic system need to be considered.

The scenarios described in this example illustrate the necessary verification activities to manage the risk of the use of the system.

9 Appendix 2 – System Description

EU Annex 11 [17] states:

> *"For critical systems, an up to date system description detailing the arrangements, data flows, and interfaces with other systems or processes, software pre-requisites, and security measures should be available"*

It is good practice to have a system description (or equivalent) for all GxP regulated systems. This may be covered by the User Requirements Specification (URS) or Functional Specification (FS), or a separate system description document may be produced.

A system description typically contains a non-technical description of the system and may include information on the business use of the system, system interfaces, and key personnel. A system description is a good introduction for laboratory scientists to a system, as well as enabling the business to demonstrate system and process understanding and control of the system.

A detailed system description is not typically necessary for very simple systems or systems with a low risk to data integrity, product quality, or patient safety. The level of detail should be commensurate with risk and complexity of the system (see Appendix D6 of GAMP® 5 [1] for further information).

Where a more detailed system description is required or helpful (e.g., in the absence of other specification documents for a complex and high risk system), the following may be considered for inclusion.

1. System identification information
    a. System name
    b. System acronym
    c. System id reference
    d. Major application software name(s) and version number(s)
    e. Operating system and service pack
2. System overview including:
    a. High level system diagram showing major system architecture and hardware, including interfaces, where applicable, to other laboratory computerized systems and attached instrumentation
    b. High level description of system functionality
        i. High level flowchart/diagram showing the functions implemented in the system
    c. Business process overview
        i. Process automated by the system
        ii. Principal roles of users of the system
    d. Sites and departments using the system and description of how the system is being used
    e. Physical location of the components

f. Network access to the system and access control (e.g., user types, user groups, and corresponding access privileges)

g. Data flow

h. Interfaces with other systems or processes

i. Description of external system interfaces, including what data are exchanged, the direction of the data flow, and the triggers for the data exchange

j. Hardware

k. Description of data managed by the system

3. Key system personnel

a. Process owner

b. System owner

c. Subject matter expert

d. User

e. System administrator

f. Database system administrator, if applicable

g. Quality control and quality assurance

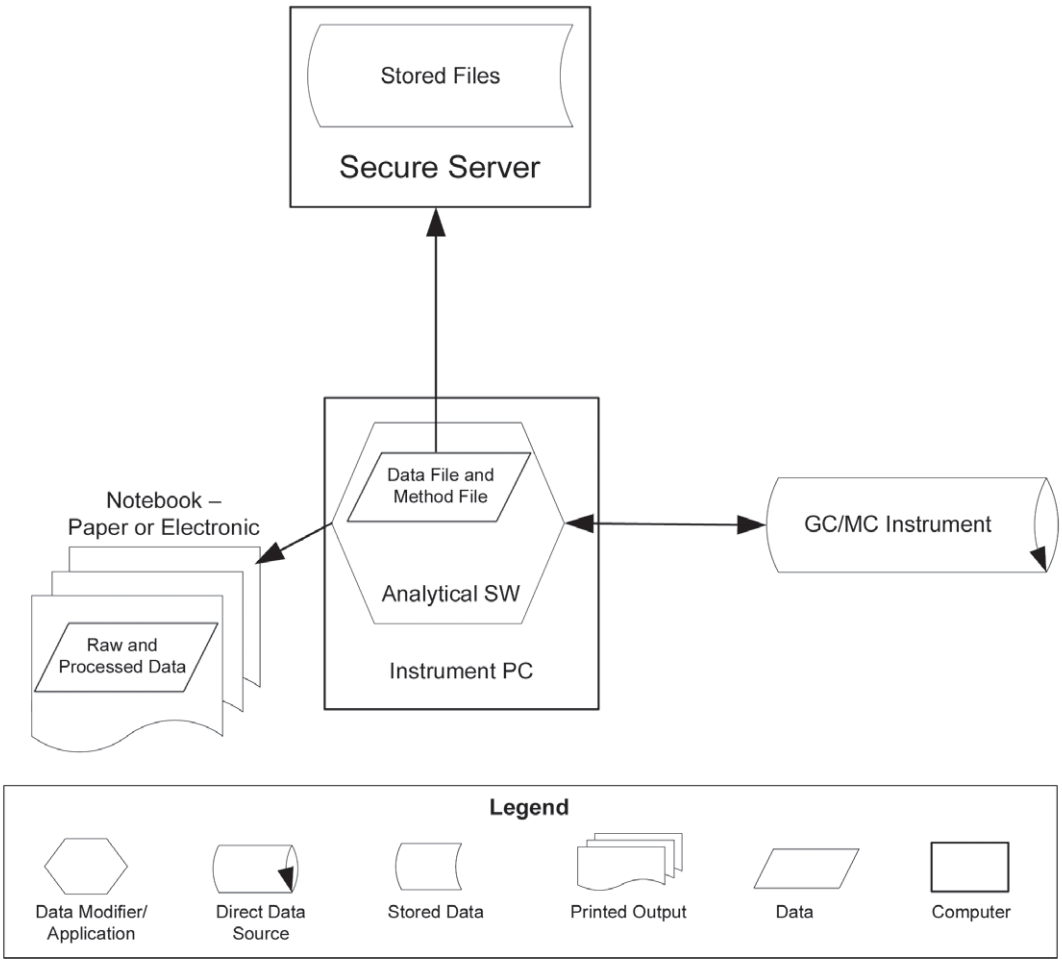
h. IT support

i. Other roles as defined within the organization

Note: some of the information listed above may already exist in other documents, e.g., system inventory, Master Configuration Item List (MCIL) validation documentation, and laboratory procedures. The system description may reference where each item of information is available, rather than repeat much of the same information in a system description.

Figures 9.1 to 9.3 provide examples of the types of system overview diagrams for commonly used laboratory computerized systems and laboratory processes.

Figure 9.1: An Example of System Overview Diagram for Process and Data Flow of a GC/MS

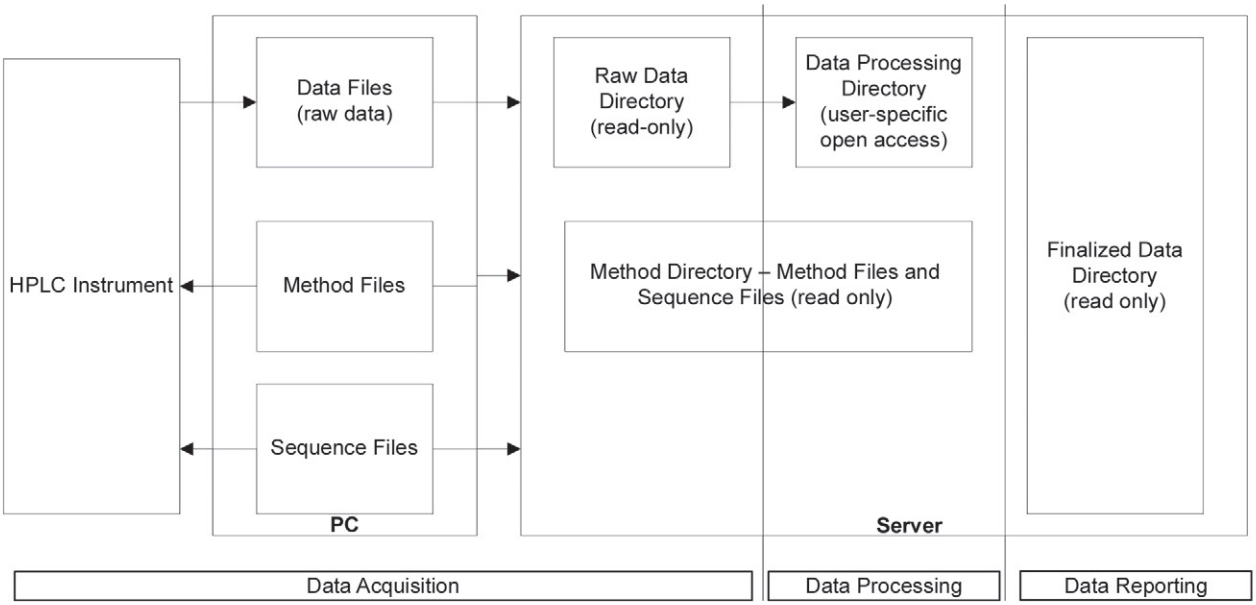


The following lists the files required to initiate a run on the GC/MS or are a result of the instrument system run:

1. **Method files** – method files control data acquisition and the various components of the instrument system

2. **Raw data files** (includes processed data) – data files are directly generated by the instrument system after a run. Limited processing is done on raw data file on the instrument PC using a method processing utility provided within the analytical software. Both the raw data and the processed data are saved in the same data file. This data file is stored on the hard drive of the instrument PC and is transferred to the secure server after the run.

Figure 9.2: An Example of System Overview Diagram for Process and Data Flow of a HPLC



The HPLC instrument system uses a PC to control the modular instrumentation. Each system may be slightly different depending on which modules comprise the system.

The common elements are:

- Personal Computer (PC)
- Automatic Liquid Sampler (ALS)
- Quaternary Pump (QP)

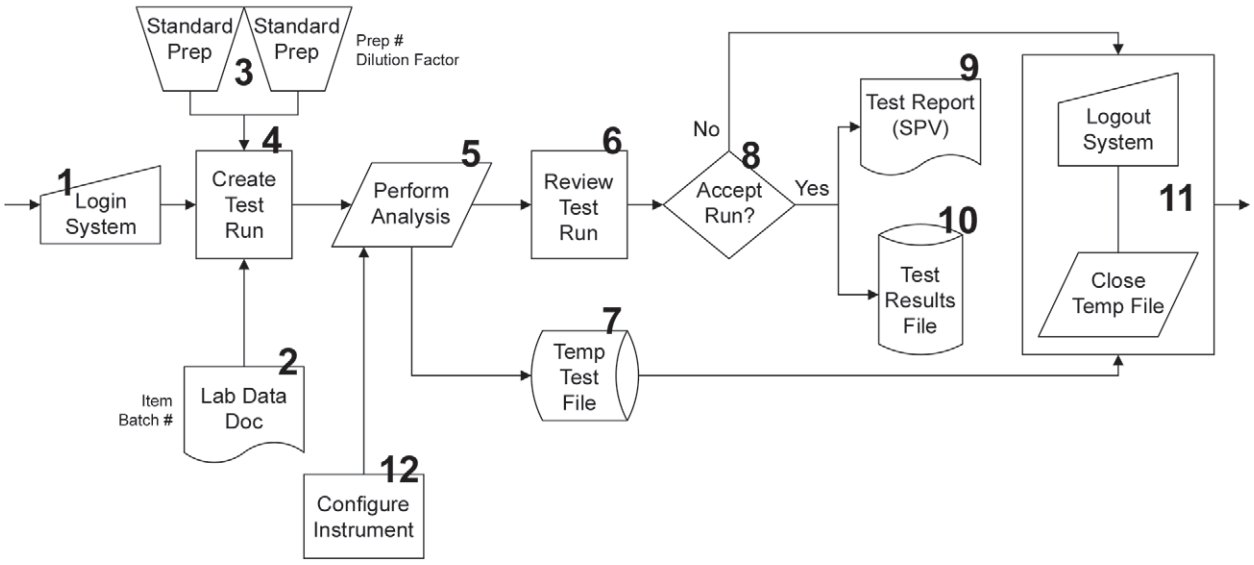
Other elements:

- Thermostatted Column Compartment (TCC)
- Thermostatted ALS
- Flowmeter
- Thermostatted Well Plate sampler (TWP)
- Bioanalyzer
- Binary Pump (BP)
- Control module (CM)
- Degassers (DG)

One or more detector modules complete the system. System operators can add or remove detection modules through change control procedures. The following lists the types of detector modules that can be connected to each system:

- Common Detection Modules:
  - Diode Array Detectors (DAD)
- Other Detection Modules
  - Multi-Wavelength Detectors (MWD)
  - Variable Wavelength Detectors (VWD)
  - Refractive Index Detectors (RI)
  - Fluorescence Detectors (FLD)
  - Mass Spectrophotometer Detector (MSD)

Figure 9.3: An Example of System Overview Diagram for Process and Data Flow of Analysis of an Analytical Sample HPLC



	1	2	3	4	5	6	7	8	9	10	11	12
Where	Lab PC	Lab Bench	Lab Bench	Lab PC Software	Lab PC Software	PC Software	Lab PC	Lab PC Software	Lab Printer	Server inntgxp01	Lab PC	Lab PC Software
Who	User, Power User, Admin	User, Power User	User, Power User	User, Power User	User, Power User	User, Power User	System	User, Power User	User, Power User	User, Power User	User, Power User, Admin	Power User
Activity	Sample is received and logged into system	Information from documentation entered into instrument set up files	Sample is fortified and extracted	Analytical method and sequence table set up on instrument	Sample and standards run on instrument	Results of sample set reviewed						
	Decision to accept or not accept analytical results	Accepted results printed	Results are saved to instrument	User logs out of instrument and closes data files	Instrument is configure as per method							

10 Appendix 3 – Data Integrity

10.1 Introduction

Data integrity is defined as "the degree to which a collection of data is complete, consistent, and accurate" [1]. The European Medicines Agency describes data integrity in terms of its characteristics, including:

- Accurate
- Legible
- Contemporaneous
- Original
- Attributable
- Complete
- Consistent
- Enduring
- Available when needed

Data integrity provides objective evidence that laboratory test results are reliable, authentic, and have not been corrupted since their creation. Data integrity is a combination of activities that occur throughout the information lifecycle, beginning at project definition and concluding at information disposal. Failure to first understand the regulations and business processes, then require, design, test, maintain, and review critical records can result in data of questionable authenticity, and may lead to regulatory, civil, or criminal action. Ensuring the integrity of critical data and metadata is necessary for all laboratory computerized systems. Within the laboratory environment, test result sets (final results and replicates), both unrounded and rounded to various levels of precision (e.g., method precision, specification precision) and audit trails of system configuration and any test run processing/reprocessing actions are examples of common critical data and metadata that defend the veracity of laboratory analyses.

"Raw data," "electronic records," and "metadata" depend upon their context within laboratory processes.

For further information see Appendix 9.

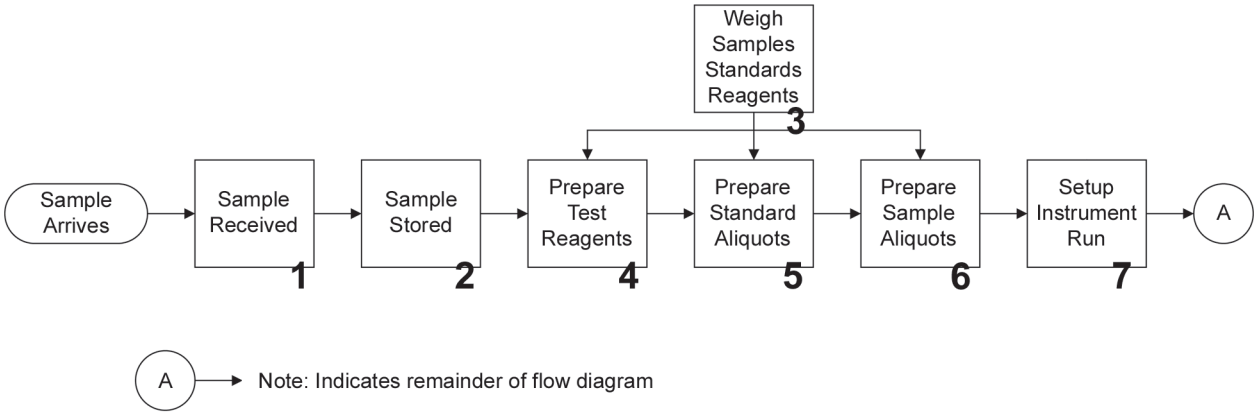
10.2 Critical Success Factors

10.2.1 Business Process and Data Understanding (System Overview)

Data integrity cannot be achieved without a complete understanding of the information flow that occurs prior to, during, and after the performance of each analytical method. This information flow provides the background for risk management of the records, highlighting parts of the process where information can be reprocessed, modified without saving, or even deleted without approval.

A data flow diagram is a useful tool to document the business process and capture all information movement. This diagram provides a visual view of the business process with the associated information that supports it. Once the diagram is created, additional attributes to specify access controls for use or modification, data storage locations, and audit trails can be added, as in Figure 10.1. These additional attributes become inputs to security role definitions, system configuration, and risk management. This is a business activity, and should be led by someone with significant understanding of the business practices. This step answers, "what information needs to be managed when executing the business process?"

Figure 10.1: Partial Generic Data Flow Diagram Example



Step #	1	2	3	4	5	6	7
Where captured?	LIMS – Receipt	LIMS – Storage	Balance to LIMS	Lab Notebook	Lab Notebook	Lab Notebook	LIMS – Execute Run
Data	Batch, Lot, Received By, Date	Sample ID, Location, Date	Sample Prep ID, Date, Number, UOM	Lots, Weights, confirmation test	Std Lot, Weight, % Moisture, Potency	Sample ID, Weights	Sample IDs, Analyst, Date, Dilution Factors, Std Potency, Configuration Method
Doer?	Analyst	Analyst	Analyst	Analyst	Analyst	Analyst	Analyst
Modifier?	(none)	Analyst	Analyst	Analyst	Analyst	Analyst	Analyst, Power User
Reviewed?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit Trail?	Yes	Yes	Yes (in LIMS)	No	No	No	No
Source Data	LIMS dB Sample Hist	LIMS dB Sample Storage	LIMS dB	Notebook	Notebook	Notebook	LIMS
Notes			Calibration in Logbook				Analyst cannot modify configuration method

10.2.2 Capability Review of Computerized System

After creating a data flow diagram of the business process, the next step is a review of the (potential) purchased system. The outcome of this review should be an understanding of system capabilities, including configuration options, audit trails, data storage locations, and storage format (e.g., text files or relational database) and access controls. It is important to identify potential data integrity issues, e.g.:

- Segregation of role conflict, for example a user can both generate and modify test results or have administrator and analyst privileges

- System requires write access to data storage area to execute test method, but as a consequence grants users permission to delete/modify files after test execution is complete

- Operating system or file manager can be used to review and delete/modify test results after test execution

- Test data or metadata is stored in text files

- Test data or metadata is stored in text files – text files are easier to delete than database records

This capability review should be led by someone with equipment or IT expertise. This is where ideas for system configuration will typically begin to form. This step answers, "what information can be managed by this system, if configured for our use?"

10.2.3 Identification of Integrity Gaps and Risk Management

Comparing the information flow (data flow diagram), that is, what is needed, with the capabilities of the system, that is, what is available – will facilitate identifying gaps that need to be addressed. The gaps will fall into one or more of the following conditions:

- Data flow diagram is not complete – an information step is missing in the data flow diagram. This requires an update of the diagram.

- Information needed for the method is missing from the system, e.g., critical sample, reagent or standard attributes, or a missing audit trail to record information re-processing.

- System manages information not needed for the method. In this scenario, the system has attributes or audit trails not necessary for method execution. This requires a plan of action to assure that users will not take action on this information. The plan might include use of security to disable access or training to raise awareness. The decided course of action should be based on the risks from using this extraneous data.

- System has some – but not all – needed capabilities. For example, this might be an audit trail that occurs in the correct place, but fails to capture a change reason from the user before creating an audit trail entry.

All identified gaps should be documented and mitigated as part of the system risk management. Mitigation should attempt to reduce the residual risks to acceptable levels, and the residual risks should be documented as part of risk management.

10.2.4 System Requirements and Design (Configuration)

The data flow diagram is an important source document when creating requirements for the system. Access controls, configuration options, data modification capabilities, and records for review and archive are all system requirements derived to some degree from the diagram. Because data integrity directly impacts GxP and business decisions, it is recommended that a section of the validation plan be devoted specifically to data integrity and security.

In laboratory computerized systems of medium complexity (or greater), appropriate configuration is crucial to achieving data integrity that is adequate for the intended use of the system. This includes application software, infrastructure, and servers. The configuration choices – and their rationale – must be carefully documented to ensure continued compliance. In situations where specific configuration choices might create undesirable effects, those choices and their impact should be included in the configuration rationale to prevent future maintenance personnel (who may be less knowledgeable) from selecting such undesirable configurations.

10.2.5 Data Review

For each laboratory computerized system, reviewers must know the location of all original data, including audit trails that indicate important changes made to source data after the initial test execution. It is imperative that all source data (and critical metadata) be thoroughly reviewed before test results are released to make decisions that impact patient safety. Reviewers must have sufficient experience with their methods and established business practices to recognize the difference between data changes made for legitimate business reasons and unusual changes that should be investigated prior to test result release. In addition to reviewing method-related data, reviewers must look at date/time stamps and other metadata, to verify a flow of business activities that are sequenced properly and are reasonable for the method. For example, a series of InfraRed (IR) scans made 10 minutes apart in a system are cause for investigation if a nominal sample preparation time is 15 minutes. Instrument use logs and lab notebooks could be reviewed to defend the authenticity of suspicious scans. Quality assurance personnel should have system accounts granting them view access to all source data so they can perform data reviews and inspections as periodically needed.

Electronic records provide the laboratory with a wealth of information about samples, methods, and personnel not available from paper records and thereby enhance the integrity of test results, when the relevant information is carefully reviewed by qualified personnel.

10.2.6 Training

Data integrity begins with training. No information system is secure without good practices and alert personnel who inform appropriate people when something looks improper. Laboratory personnel and quality assurance should be taught where they can find the list of critical and relevant records for any method in their area. Personnel should be aware of proper segregation of duties and/or potential conflicts of interest in their assigned roles, and how to procedurally address them. Human factors that contribute to testing errors and data fraud should be clearly understood along with tools/techniques for examining test data and metadata. Depending on the method, users may require training to avoid certain system features that are unnecessary for method execution.

10.2.7 Designing for Integrity

Current laboratory computerized systems offer a limited set of configuration choices ranging from very simple – setting a file storage directory, to moderately complex – selecting user actions that will create an audit trail entry. As discussed above, systematic understanding of the business and data during the implementation phase can result in a configuration optimized for the intended use with known data integrity risks that are mitigated to a reasonable level of compliance.

While it is acknowledged that most current systems present a limited configuration, as laboratory computerized systems evolve, greater flexibility will permit design decisions that maintain a high level of data integrity while they also increase efficiency and reduce human error in operations. Current systems require reviewers to visually inspect audit trails before test result release. Efficiencies will be derived when electronic systems are capable of notifying users/reviewers when added attention should be focused on a record. For example:

- Software raises a warning when test results are re-processed after test execution. For example, chromatography peaks change their labels when peaks are manually positioned so reviewers distinguish manual baselines from automated ones.
- Report view lists the data source file when a report is copied from an existing test run.
- Software raises a warning when audit trail records do not have successive chronology.
- Software periodically scans test result folder and raises a warning when result files are missing.

These illustrate a small sample of capabilities that will improve integrity and efficiency, helping personnel to review data/metadata where needed.

11 Appendix 4 – Simple Systems

Simple systems are laboratory computerized systems that are composed of non-configurable components which generate a numeric value based on their firmware. Examples include:

- Standalone balances (not interfaced to a computerized system)
- pH meters
- Pipettes

Simple systems require the application of sound scientific principles to their specification, verification, and operation. Traceable standards should be used to assure measurement accuracy and precision.

Depending on their use, simple systems may become sufficiently complex to be considered medium systems, e.g., programmable pipettes with a set draw and dispense rate for viscous fluids.

Tables 11.1 to 11.16 provide a guideline for verification activities of simple systems. These activities should be selected to meet the needs of the system in accordance with its intended use in the laboratory. Some of these activities may not be required. Activities may involve only simple checklists or forms.

Note: the tables in this appendix indicate typical roles which may be involved in each activity. The extent of the involvement of Quality Control (QC) and Quality Assurance (QA) depends upon the GxP impact and an organization's quality management processes and procedures.

11.1 Generic Activities for Simple Systems

Table 11.1: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify need and system requirements (including operating range(s), safety and environment)	Process Owner System Owner User Business Management	Specification document	Key to ensuring compliance with business and regulatory requirements

Table 11.2: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select the system	System Owner User Supplier Quality Control and/or Quality Assurance	Manufacturer's literature Catalogues Evaluation notes based on initial specification Update specification document, if appropriate	Review manufacturer's literature Consult other expert users to ensure instrument is fit for intended use Hands on evaluation of instrument, if appropriate Note: system owner and end user may be same person throughout this process due to the relative simplicity of the system.
2. Place purchase order	Purchasing Department	Purchase order Warranty Service contact	
3. Receive system	Process Owner User Supplier	Place on system inventory list	Check delivery note versus purchase order to ensure correctness and completeness
4. Inspection verification	Process Owner User Supplier	Installation specifications, including services, safety and environment, and performance, as necessary Installation verification document Supplier documentation (e.g., user manual, factory testing and calibration certificates if appropriate)	May use generic installation checklist Can use available vendor documentation subject to pre and post execution review and approval Initial factory calibration certifications and other documentation shall be captured and saved for reference.
5. Conduct safety assessment	Process Owner User Quality Control and/or Quality Assurance Safety Department Supplier	Company-specific Regional regulatory documentation may also be required (e.g., Control of substances hazardous to health)	

Table 11.2: Project Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
6. Conduct environmental checks	User Supplier	Supplier documentation (e.g., user manual, installation specifications, performance requirements)	Ensure environment for instrument
7. Training	Process Owner User Supplier	System use SOP Training materials Training records	Should cover use, maintenance, calibration, and documentation requirements
8. Establish acceptance criteria based on specifications and conduct verification tests	User Process Owner Supplier Support Staff (e.g., Calibration)	Testing plan or protocol using traceable standards as necessary Documented evidence of testing Release system for operational use document	Designed to confirm that specifications have been met and that instrument functions as specified under normal operation and realistic stress conditions Use materials traceable to national or international standards where available May follow standard form or template May perform instrument diagnostics or self-test compared with traceable standards

Table 11.3: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Place into operational use	System Owner Quality Control and/or Quality Assurance	Change control or release statement depending upon company policies Maintenance/use log	Documentation based on regulatory requirements
2. Establish and ensure continued performance	System Owner User Supplier	Instrument SOP updated Maintenance/use log Service contract Calibration schedule	Ensure calibration and maintenance are established. This may be conducted internally or via second or third party suppliers and should be performed on a predetermined periodic interval (e.g., every six months' calibration to meet acceptance criteria).
3. Change management, incidents/problems	System Owner User Supplier Quality Control and/or Quality Assurance	Maintenance/use log Deviation management and CAPA	May need to re-establish acceptance criteria (e.g., moving non-portable instrument to new location)

Table 11.4: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify instrument/ components to retire	System Owner Archivist or equivalent Quality Control and/or Quality Assurance	Take instrument out of operational use Archive SOP and maintenance/use log	Cancel maintenance or calibration schedule Archive all instrument maintenance/use log, manuals, etc. Cancel maintenance contracts
2. Disposal of instrument	Process Owner	Document disposal	Part of decommissioning may also include system decontamination and disposal according to regulatory requirements.

Subsequent sections in this appendix provide examples of activities for simple systems. Choose them such as they meet system needs according to the intended use in the laboratory. Depending on the unique implementation of each system, the information presented may/may not be needed.

11.2 Example 1 – Analytical Balance

This example is for an analytical balance used in a GxP laboratory that is not connected to a computerized system, e.g., ELN or LIMS. When working to GMP regulations, regional pharmacopeial requirements should be added.

If connection to a computerized system is needed, this should be included in the user requirements. As analytical balances are becoming more sophisticated, there also may be requirements for the balance to act as a terminal for the computerized system it is interfaced with and the associated user interactions during weighing.

Table 11.5: Concept Phase

User requirements should be defined for simple systems, as demonstrated in Table 11.5. An analytical balance is usually a critical item of instrumentation which cam impact all analyses in a laboratory.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify need and system requirements	Process Owner User	User specification	Define operational range of the balance plus the requirements for precision and accuracy. Include regional Pharmacopoeial requirements as necessary. Define any calculations to be performed by the balance, e.g., tare weight, content uniformity, loss on drying. Local printer connected to the balance for documenting the output of the balance Location of the balance and impact of vibration: laboratory or slate bench. Understand the materials to be weighed and if they are toxic or hazardous (e.g., does the instrument need to be housed in a glove box?) or will statically charged or friable materials be weighed? Consider protection from drafts, e.g., air ducts, laboratory thoroughfares. Temperature and relative humidity of the laboratory.

Table 11.6: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select best system, evaluate balances with printers versus user specification	Process Owner User Supplier Quality Control and/or Quality Assurance	Supplier literature and warranty documentation Evaluation notes	Review supplier web sites. Review supplier literature and warranty information. Arrange on site demonstration and evaluation, if appropriate. Evaluation notes and selection versus user specification.
2. Place order	Purchasing Department	Purchase order	
3. Receive instrument	User	Place on instrument inventory list Reconcile order versus delivery note	
4. Installation verification	Process Owner User Supplier	Installation verification document Supplier manuals Supplier certificates of manufacture and factory calibration of balance Certificates of masses used to calibrate balance	Review supplier installation verification document and approve pre-execution. Install, connect to services, ensure level, eccentricity, hysteresis, etc. to verify correct installation. Supplier or third party uses external masses traceable to national standards. Confirm environmental conditions as acceptable. Review and approve installation verification.
5. Training	Process Owner User Quality Control and/or Quality Assurance	Instrument SOP Maintenance/use log	Define proper use and develop SOP maintenance procedures. Routine calibration defined: internal versus external calibration.

Table 11.6: Project Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
6. User acceptance testing	Process Owner User Quality Control and/or Quality Assurance	User acceptance testing documentation and release for operational use Calibration certificates of external masses used Instrument SOP Maintenance/use log Release for operational use	Testing balance versus user requirements: operational range checked using F1 weights Internal check weight verified with external traceable weight Compliance with USP. Calculations verified under actual conditions of use, if appropriate.

Table 11.7: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Operational use	Process Owner User	Instrument SOP Maintenance/use log Calibration schedule Release for operational use	Cleaning instructions for balance pan, e.g., use of non-static brush. Balance should be calibrated prior to use either by using the internal check weight or external check weights. Establish calibration schedule and approach.
2. Establish and ensure continued performance	Process Owner User Supplier	Maintenance contract Certification of acceptance by supplier Trending of calibration data to detect performance issues.	Balance and all check weights should be calibrated regularly using traceable weights (typically by a qualified external supplier).
3. Change management, incidents/problems	Process Owner User Supplier	Maintenance/use log	Re-conduct part of all stages of verification if balance conditions are changed (e.g., moving to new location, firmware updated). Balance placed out of service if performance criteria are not met. Deviation management and CAPA to investigate problems and incidents.

Table 11.8: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify instrument/ components to retire	Process Owner User Archivist Safety Department	Remove from inventory list Archive SOP and Maintenance/use log Cancel maintenance contract Removal certificate	Balance no longer in use and placed out of service/ retired. Part of decommissioning also may include system decontamination and disposal according to regulatory requirements.

11.3 Example 2 – Ph Meter

This example is for a pH meter used in a GxP laboratory. The pH meter is not connected to a computerized system, e.g., ELN or LIMS, but is connected to a local dedicated printer. The pH meter is intended for general purpose laboratory use, as well as for making measurements for batch release purposes.

Table 11.9: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify need and system requirements	Process Owner User	User specification	Define operational range of pH measurement. Define measurement precision and accuracy. Define electrode type and number of calibration points (2 – 4). Define if temperature compensation is required. Define if autosensing calibration is to be used. Define if calibration solutions are to be used over the operating range. Specify environmental conditions.

Table 11.10: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select best system	Process Owner User Supplier Quality Control and/or Quality Assurance	Manufacturer's literature Selection of the system versus user requirements	Supplier web sites Warranty documentation
2. Place order	Purchasing Department	Purchase order	
3. Receive instrument	User	Place on instrument inventory list	Check delivery note versus purchase order.
4. Installation verification	Process Owner User Supplier	Supplier's user manual Calibration certificates for pH solutions used Installation verification document	Generate and approve installation verification document or review and approve supplier installation document. Place on laboratory bench and connect components. Confirm that pH meter works using calibrated pH solutions.
5. Conduct safety assessment	User Safety Department	Safety checklist	
6. Training	Process Owner User Quality Control and/or Quality Assurance	Operating manual Instrument SOP	Maintenance procedures Routine calibration
7. User acceptance testing	Process Owner User Quality Control and/or Quality Assurance	Instrument SOP Maintenance/use log User acceptance testing Calibration certificates of pH solution used Release for operational use	Check if installation verification testing covered operational range in user requirements. If yes, release system for operational use. If no, plan additional testing to cover working range and accuracy/ precision. Release system for operational use

Table 11.11: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Operational use	Process Owner User	Instrument SOP Maintenance/use log	
2. Establish and ensure continued performance	User Supplier	Maintenance/use log Calibration schedule Maintenance contract Certification of acceptance by supplier	Follow acceptance criteria to ensure continual performance. Immerse electrode head in neutral buffer solution when not in use. Trending of results over time.
3. Change management, incidents/problems	Process Owner User Supplier	Maintenance/use log	Re-conduct acceptance criteria if instrument is moved to different laboratory or if components are changed (e.g., new electrode). Place out of service if performance criteria not met: Deviation Management and CAPA.

Table 11.12: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify instrument/ components to retire	Process Owner User Archivist Safety Department	Remove from inventory Archive SOP and Maintenance/use log Cancel maintenance contract Removal certificate	pH meter no longer in use and placed out of service/ retired. Part of decommissioning also may include system decontamination and disposal according to regulatory requirements.

11.4 Example 3 – Electronic Pipette

This example is for an electronic pipette used in a GxP laboratory for dispensing and diluting standard and sample solutions for batch release purposes.

Table 11.13: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify need and system requirements	Process Owner User Quality Control and/or Quality Assurance	User requirements	Pipette to measure either single volume or range of adjustable volumes. Single or multiple simultaneous dispensing required. Limited program capability, e.g., intakes 1 ml and dispenses 200 µl repetitively. Establish acceptance criteria.

Table 11.14: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select best system	Process Owner User Supplier Quality Control and/or Quality Assurance	Supplier literature	Supplier internet sites Request warranty documentation
2. Place order	Purchasing Department	Purchase order	
3. Receive instrument, mount identification sticker	User	Place on inventory list	
4. Installation verification	Process Owner User Supplier	Operating manual Calibration certificate of pipette	
5. Training	Process Owner User Quality Control and/or Quality Assurance	Operating manual Instrument SOP	Proper use Maintenance procedures Routine calibration

Table 11.15: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Operational use	Process Owner User	Instrument SOP Maintenance/use log	Define regular calibration frequency and acceptance criteria
2. Establish and ensure continued performance	Process Owner User System Supplier Supplier	Maintenance/use log Calibration schedule Maintenance contract Certification of acceptance by supplier	Check pipette volumes (daily use) and assure predetermined calibration scheduled
3. Change management, incidents/problems	User Supplier	Maintenance/use log	Pipette is placed out of service if performance criteria are not met. If the pipette can be repaired, send pipette for repairs and calibrate before returning to use.

Table 11.16: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify instrument/ components to retire	Process Owner User Archivist Safety Department	Remove from inventory Archive SOP (depending on if not needed for other instrument or GxP regulations) and maintenance/use log Disposal certificate	Electronic pipette no longer in use and placed out of service/retired. Part of decommissioning also may include system decontamination and disposal according to regulatory requirements.

12 Appendix 5 – Medium Systems

Medium systems are laboratory computerized systems that are typically composed of configurable components which generate a value based on their firmware and with software which has discrete configuration capabilities. Examples include:

- Bench top spectrophotometers
- Capillary electrophoresis
- Polymerase Chain Reaction (PCR) cyclers
- Near-Infrared Spectroscopy (NIR)
- Fourier Transform Infrared spectroscopy (FTIR)
- High-Performance Liquid Chromatography (HPLC) and Gas Chromatography (GC) instruments connected to an external system

12.1 Scope of Activities When Connected to an External System

Medium systems may be connected to an external software system, such as a Chromatography Data System (CDS) or Electronic Lab Notebook (ELN). Where possible, activities to demonstrate that the external software system is fit for intended use should be completed separately to avoid excessive project complexity.

The laboratory computerized system scope ends at the data port, but should include verification of instrument control files downloaded by the external software system. The files should be verified before test initiation and should be uploaded to the external software system after testing. This approach is intended to simplify the addition or removal of systems from external software systems, where adding or removing systems has been performed within the scope of the external software system processes.

Tables 12.1 to 12.7 provide a guideline for activities, which may be used for medium systems. They are based upon an HPLC connected to a CDS. These activities should be selected to meet the needs of the instrument in accordance with its intended use in the laboratory. Some of these activities may not be required. Activities may involve only simple checklists or forms.

Note: the tables in this appendix indicate typical roles which may be involved in each activity. The extent of the involvement of Quality Control (QC) and Quality Assurance (QA) depends upon the GxP impact and an organization's quality management processes and procedures.

12.2 Generic Activities for Medium Systems

Table 12.1: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify need and system requirements	Process Owner IT Representative Quality Control and/or Quality Assurance	Statement of intended use Functional requirements Roles and responsibilities	Requirements are needed for objective evaluation of systems. Define needed security roles and their functions in the business process prior to functional requirements. Quality Control and/or Quality Assurance verifies that all regulatory requirements are met.

Table 12.2: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select best system	Process Owner System Owner Supplier IT Representative	Catalogues Specification documentation Design verification (Identify unmet requirements and gaps in data integrity) Design requirement (if connected to remote data storage) Supplier assessment Risk assessment	Consult web, conduct verbal recommendations, etc., to ensure system is fit for intended use. Use risks to decide proper type of audit: remote or on-site.
2. Place order	Purchasing Department	Purchase order Warranty Service level agreements (Critical spare parts, if needed)	Critical spare parts can be an issue if business depends on system availability.

The verification activities of the project phase may be structured as separate stages covering installation, operation, and performance.

Verification should include receipt of ordered items including:

- Manuals
- Support materials
- Software drivers
- Any equipment spare parts

The operation of individual components across the specified range should be verified; where possible, supplier documentation should be used. System performance should be verified based on the intended use of the system.

Note: system-specific checklists may be used for verification activities.

Table 12.3: Project Phase (Installation Verification Stage)

Activity	Personnel	Deliverables/ Documentation	Comments
1. Receive system	System Owner User Supplier	Place on equipment inventory list	
2. Inspection of system and components	System Owner Supplier IT Representative	Supplier documentation (e.g., user manual, installation specifications, performance requirements)	Consider use of installation checklist, for greater documentation efficiency.
3. Conduct safety assessment	System Owner Safety Department	Company-specific	
4. Conduct environmental checks	System Owner Supplier	Supplier documentation (e.g., user manual, installation specifications, performance requirements)	Confirm appropriate environment before use. Environment can be critical for systems determining moisture content.
5. Verify system connections to data and utilities	System Owner Supplier IT Representative	Supplier documentation Design requirements for data storage	Facility modifications made prior to installation. Verify data connection is functional. Data transfer verified in performance verification stage.
6. Establish Preventive Maintenance procedures	System Owner Engineering Quality Control and/or Quality Assurance	Preventive Maintenance schedules and protocols Supplier documentation	Verify range of use, specifically, if supplier protocols are used.
7. Establish documentation repository	System Owner Quality Control and/or Quality Assurance	Equipment files or records	Collect and retain documentation to support the system through its life cycle.
8. Training (Note: in some situations, this should occur prior to Operational Verification)	Process Owner System Owner Administrators End User Maintenance personnel Supplier	Training plan Training records (depending upon GxP and organization policies)	Should cover use, security, maintenance, calibration, and documentation requirements.

Table 12.4: Project Phase (Operational Verification Stage)

Activity	Personnel	Deliverables/ Documentation	Comments
1. Establish acceptance criteria for Operational Verification Stage	Process Owner System Owner Supplier SME	Traceability of requirements and tests Test execution process Testing documentation Managing test failures Test scripts Configuration control process Test data, as needed Test protocols	Consider use of checklist, for greater documentation efficiency. Note: system should be visibly identified as out of service.
2. Establish and document system configuration	System Owner Supplier	Configuration list	Sets the baseline for system configuration and support. Includes software and hardware options selected.
3. If applicable, calibrate components and perform modules tests (e.g., detector wavelength accuracy, detector linearity, noise and drift, pump flow precision, injector precision, injector carryover, column temperature, gradient accuracy)	System Owner Supplier Support staff (e.g., Calibration) User	Completed test protocols Calibration report (as found, as left) Test failure report(s) Supplier Qualification document(s)	Sequence of tests could be important. Supplier Qualification documents may be leveraged to support operating parameter verification.
4. If not completed, configure system security	Administrator	Access Roster	Sometimes done prior to module tests, but should be finished prior to performance verification stage.

Table 12.5: Project Phase (Performance Verification Stage)

Activity	Personnel	Deliverables/ Documentation	Comments
1. Finalize system procedures (use, administration)	Process Owner System Owner Administrator	System SOP Access Control SOP	Procedures should be followed during test protocol(s).
2. Establish acceptance criteria for verification protocol and security tests	Process Owner System Owner SME	Test protocol	
3. Complete security configuration tests	Process Owner System Owner Administrator	Completed protocol	Challenge access to system, configuration, and any remote data storage areas.
4. Complete tests	Process Owner System Owner	Completed protocol	Tests will vary by intended use and data storage. Should include verification of correct data files into a validated CDS.
5. Complete quality review	Process Owner System Owner Quality Control and/or Quality Assurance	Quality report	Review of all activities and open issues prior to first use in production.

Table 12.6: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Place into use	Process Owner System Owner User	Instrument SOP – depending upon company policies and GxP Maintenance/use log	Documentation based on regulation requirements.
2. Establish and ensure continued performance	Process Owner System Owner Supplier	System SOP – depending upon company policies and GxP Maintenance/use log Maintenance contract Calibration schedule Contract for system upgrades, etc.	Ensure calibration and maintenance are established and in-place – may be conducted internally or via second party supplier.
3. Execute Change management, incidents/problems	Process Owner System Owner Quality Control and/or Quality Assurance User	Maintenance/use log	May need to re-establish acceptance criteria (e.g., moving non-portable equipment to new location).
4. Perform Periodic Reviews	Process Owner System Owner Quality Control and/or Quality Assurance	Periodic review report	Review incidents, access roster, security issues, looking for trends in performance.

Table 12.7: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Create Decommissioning (Retirement) Plan	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Retirement/migration plan	Specifies destination of system, procedures, and data.
2. Identify system/ components to retire	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Archival of equipment SOP (depending on GxP regulations) Maintenance/use log	Remove from inventory. Part of decommissioning also may include system decontamination and disposal according to regulatory requirements. Cancel maintenance or calibration schedule.
3. Identify records to migrate or retire	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Migration or retirement plan	
4. Migrate data and/or retire system per plan	System Owner IT Representative Quality Control and/or Quality Assurance	Verification documents	If data are migrated to a new system, records of the migration need to be generated to demonstrate that the records have not changed content or meaning.
5. Create Decommissioning Report	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Retirement/migration report	Reviews activities performed.
6. Remove support materials and spare parts from active inventory	System Owner	Remove/retire SOPs, manuals, logbooks	Prevents use of retired materials.
7. If retired system is kept for data access, perform Periodic Review(s)	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Periodic review report	Review access roster, frequency of access.

13 Appendix 6 – Complex Systems

Complex systems are laboratory computerized systems that are typically composed of multiple configurable or custom components which are based upon a networked architecture.

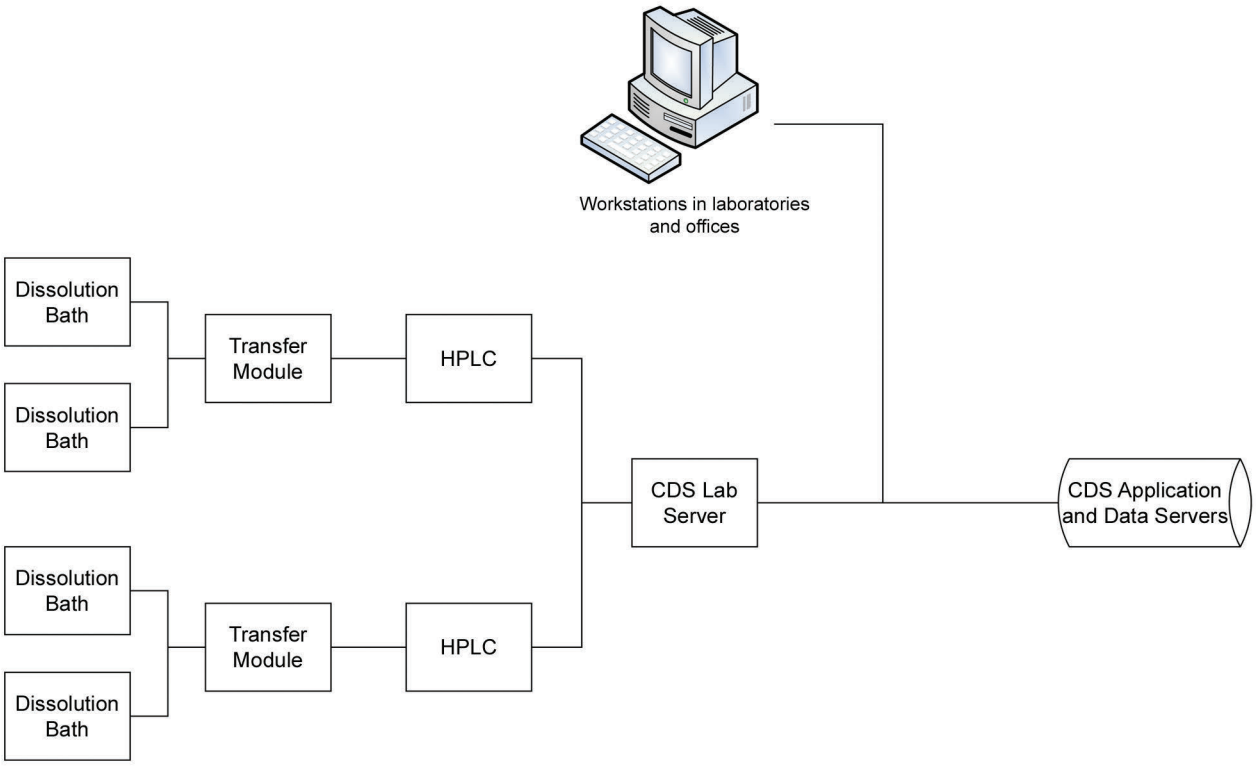
The example provided in this Appendix discusses the validation of a complex laboratory computerized system consisting of a networked Chromatography Data System (CDS) that controls, acquires, and interprets data from an automated dissolution – HPLC analysis.

The system in this example has been configured to use electronic signatures; no paper is printed out from the system; however, there is an option to print a final report.

13.1 System Architecture

Figure 13.1 shows an overview of the system architecture. Each module consists of two dissolution baths connected to a single HPLC system via a transfer module. Samples from a vessel in each dissolution bath are transferred to a vial, and then transferred to the HPLC system for analysis. Each data server can control and acquire data from up to two HPLC system modules connected to four dissolution baths. The data server also can act as a data buffer if the network or CDS server is unavailable. The CDS application and data are stored on servers located in the computer room (data center) and under control of the organization's IT function.

Figure 13.1: Automated HPLC-Dissolution System Architecture



The architecture illustrated in Figure 13.1 shows the database and application as "servers;" this can be a single server on which the database is installed and which manages the chromatographic data generated by the system. Alternatively, the system can be installed on separate servers, with one holding the database and files and another holding the CDS application. The CDS application also can be installed and managed by a terminal server application.

13.2 Multidisciplinary Approach to Validation

Validation of this system requires a multidisciplinary approach as it contains:

- Analytical systems (dissolution baths and HPLC chromatographs) managed by laboratory personnel.
- Data servers positioned in close proximity to the chromatographs they control and from which they acquire data (on the laboratory network side of the network socket) to provide resilience in case of network unavailability to buffer the data.
- Central server(s) and the network, which are operated by the IT function and consist of Category 1 software (database, operating system, and utilities) and also may have the CDS application software installed.
- Category 4 CDS application software that requires user configuration including an option for electronic signatures. This can be installed on a server or individually on each system, depending on the overall architecture.
- Ability to define specific custom calculations for individual chromatographic analyses – Category 5 software.

The CDS system under discussion is standalone and is not interfaced to another laboratory computerized system (e.g., an ELN or LIMS) or other analytical instruments (e.g., analytical balances). For further information on interfacing to other systems, see Appendix 7.

13.3 Order of Validation Activities

The subsequent sections of this Appendix list activities that lead to the validation of a large laboratory system, such as the automated CDS system. These activities are intended as guidance and individual organizational procedures may state that some tasks take place in a different order to those suggested in this Guide. Organizations may omit some activities. Organizations also may require some activities not listed in this Guide.

13.4 Validation Activities

Activities should begin with understanding current processes involving the system and streamlining the processes prior to implementation. The system selection process is based upon an initial definition of user requirements that will be used to select a system. As system functions are better understood during later project phases, requirements will likely be updated to reflect the selected system.

Tables 13.1 to 13.7 provide a guideline for activities which may be used for complex systems.

Note: the tables in this appendix indicate typical roles which may be involved in each activity. The extent of the involvement of Quality Control (QC) and Quality Assurance (QA) depends upon the GxP impact and an organization's quality management processes and procedures.

Table 13.1: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Map the analytical process and redesign it for electronic working	Process Owner User Quality Control and/or Quality Assurance IT Representative	Process mapping and redesign document Data flow diagrams Initial draft of risk management	Map and understand the current business process and data flow (see Appendix 3 on Data Integrity). Streamline for electronic working practices prior to implementation of the system. Eliminate unnecessary process activities. Identify calculations that can be included in the new system to eliminate use of spreadsheets. Start draft of risk management document.
2. Identify business need and user requirements	Process Owner User System Owner Quality Control and/or Quality Assurance	Statement of intended use Initial user requirements	Requirements are needed for objective evaluation of systems. These requirements may be influenced by regional pharmacopoeial needs. Note: these initial user requirements will need to be updated after training, prototyping, and configuration to reflect the actual system purchased and implemented.

Table 13.2: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Select system	Process Owner System Owner User Supplier Quality Control and/or Quality Assurance IT Representative	Supplier advertising literature Supplier specification and other supplier documentation Design verification (including unmet requirements and data integrity gaps) Discuss with supplier server architecture and sizing for current and future growth of the system System risk assessment Professional services offered by supplier discussed	Consult web and trade publications for potential systems and suppliers. Demonstration of system to compare with laboratory user requirements. Seek verbal recommendations from existing users to ensure that the system is fit for intended use. Understand the system requirements for the servers to run the system with input from the supplier. Will the system fit into the corporate architecture?
2. Supplier assessment	Process Owner Supplier Quality Control and/or Quality Assurance	Risk assessment to determine on-site or remote assessment Supplier assessment report	Use risk assessment to decide proper type of supplier assessment: remote or on-site. Evaluation of the supplier's quality management system for the design, development, release, and support of the CDS application software.
3. Place order	Purchasing Department	Negotiate contract terms and conditions Professional services provides by supplier for installation of components and system Final quotation and contract IT orders servers for system and additional IT equipment Purchase order Warranty	The purchase orders provide the starting point for managing the configuration of the whole system.

Table 13.2: Project Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
4. Write Validation Plan for the system	Process Owner System Owner Quality Control and/or Quality Assurance	Perform a documented risk assessment of the system use Define the scope of the system validation Define the roles and responsibilities of personnel Define the life cycle phases to be undertaken Define the documented evidence to be written	Validation Plan needs to define and control the overall validation work. Depending on the size of the system being implemented, roll-out may need to be phased.
5. Establish documentation repository	System Owner Quality Control and/or Quality Assurance	Equipment files or records	Collect and retain documentation to support the system through its life cycle.
6. Plan key user training	Process Owner System Owner Administrator User	Identify key users to be trained in basic operation of the new system and user administration Identify and train IT staff to support the system	Plan for key training early in the project to ensure the way the system works in detail is understood for prototyping the electronic process, configuring the system, and implementing custom calculations.

Several verification activities should take place during the project phase. These are described in subsequent tables in this appendix. Figure 13.2 provides a detailed overview of verification activities at each stage of the project.

The foundation of the approach is based upon component verification that consists of:

- IT Department: installation and verification of the servers, operating system, and application software
- User: installation and verification of analytical instruments and laboratory data server
- Verifying that the laboratory and IT components have been integrated correctly and work together correctly
- Prototyping of system use to determine how to configure the application software
- User acceptance testing to verify that the configured system is fit for intended use

Figure 13.2: Verification Activities from Installation of Components to User Acceptance Testing

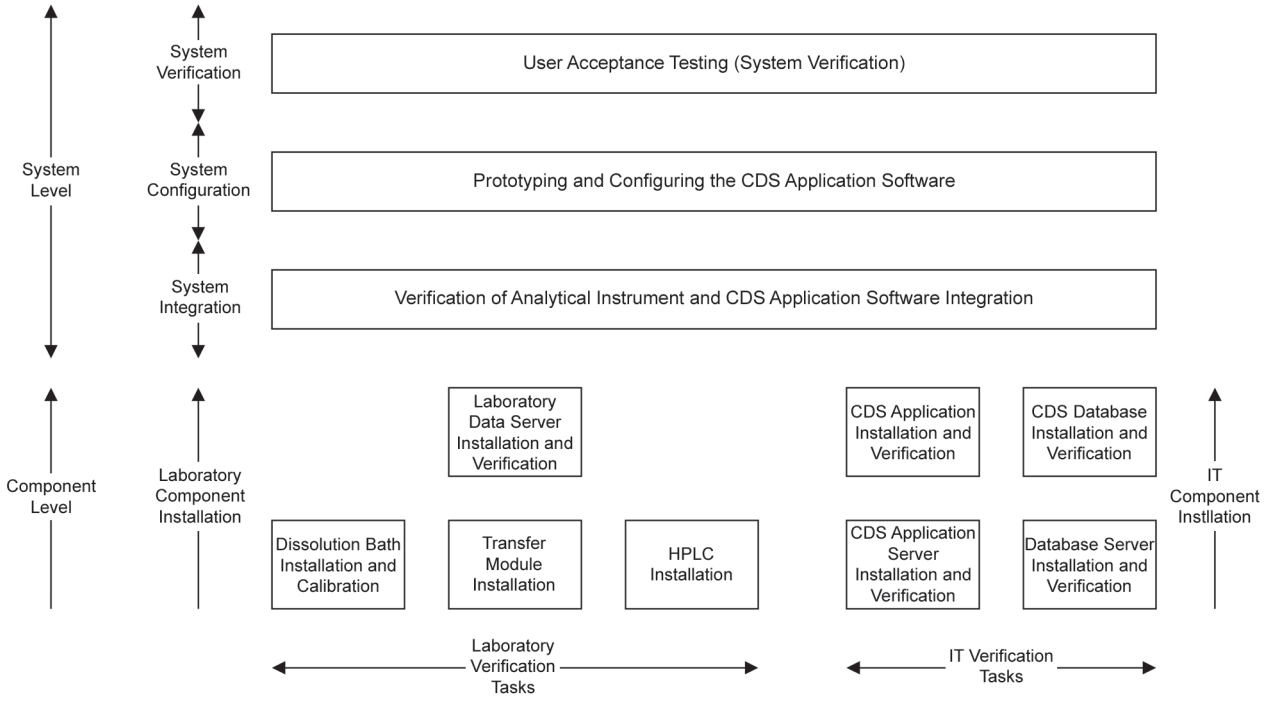


Table 13.3: Project Phase (Installation of Components and System Integration)

The project phase begins with verification that ordered items are in-house and correct, e.g., manuals and software drivers. Installation usually involves work in both a laboratory and the computer room data center. Instrument specifications may be derived from supplier documentation and in the case of the dissolution equipment, from regional pharmacopoeial requirements.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Write installation plan	User Process Owner System Owner	Installation plan	Identify where analytical instruments, data servers, etc., will be located in the laboratories. Check adequate services for the intended use of the instruments. Identify whether existing or new network connections will be used or whether additional ones need to be installed prior to installation of the system. Identify whether existing or new workstations are required for user access to the system.

Table 13.3: Project Phase (Installation of Components and System Integration) (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
2. Write technical specification	System Owner Process Owner Quality Control and/or Quality Assurance	Technical specification	The server architecture and specifications are defined in this document, e.g., terminal servers (if used), hardware for fault tolerance, service availability, and estimated downtime. This document should include definition of the production system as well as any test or training environments. IT support requirements, e.g., backup and recovery are defined here or in a Service Level Agreement (SLA).
3. Receive instruments, software and computer equipment and inspect versus purchase order	Process Owner System Owner Supplier	Check delivered versus ordered and rectify if any items missing Place on system inventory list	Supplier instruments, software, documentation (e.g., user manual). Installation specifications, performance requirements).
4. Install and qualify IT servers	Process Owner System Owner	Server verification documents	This phase covers server hardware installation, installation, and configuration of the operating system and any service packs and security patches plus any software utilities required by the IT department.
5. Install and qualify CDS database (if applicable) and application software on server(s)	Supplier System Owner Process Owner	CDS application software verification documents	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.

Table 13.3: Project Phase (Installation of Components and System Integration) (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
6. Install and qualify CDS application software on laboratory data servers	Supplier System Owner Process Owner	CDS application software verification documents	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.
7. Install and qualify CDS application software on laboratory workstations	Supplier System Owner Process Owner	CDS application software verification documents	Depending on the architecture of the system, this task may not be required. Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.
8. Install and qualify dissolution baths in laboratory	Supplier System Owner Process Owner	Verification documentation	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.
9. Install and qualify HPLCs in Laboratory using CDS application software	Supplier System Owner Process Owner	Verification documentation	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.
10. Install transfer module linking dissolution baths with an HPLC	Supplier System Owner Process Owner	Verification documentation	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.

Table 13.3: Project Phase (Installation of Components and System Integration) (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
11. Qualify the dissolution baths, transfer module and HPLC using CDS software	Supplier System Owner Process Owner	Verification documentation	Ensure scientific soundness of the supplier documentation before purchase or execution. Ensure pre- and post-execution review and approval of supplier documents.
12. Establish Preventive Maintenance procedures for analytical instruments	Process Owner Engineering Quality Control and/or Quality Assurance	PM schedules and protocols Supplier documentation	Check that the laboratories operational range of use matches the supplier protocol.
13. Establish and document system configuration: hardware, software, and instrumentation	System Owner Supplier	Configuration list	Set the baseline for system configuration and support. The scope of the configuration Includes software, hardware, and documentation. Change control and periodic reviews should be performed to demonstrate that the system is in control.
14. Summary report of installation of system components	Process Owner	Installation report	Collation and summation of the installation and integration phases of the work.

Table 13.4: Project Phase (Prototyping and Specifying Software Configuration)

This part of the verification may be performed in part on a test/validation instance of the system or completely on the operational system, depending on the resources available.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Prototype electronic working practices	Process Owner User Administrator Quality Control and/or Quality Assurance	Configuration specification	Based on the process redesign document from the concept phase, implement electronic working practices, evaluate settings for operation of the application and configuration for ensuring data integrity.
2. Configure CDS Application Software	Administrator	Configuration set-up confirmation	Based on the outcome of the prototyping, the software configuration of the operation system will be set up.
3. Configure system security: define users and allocate to user type/group with associated access privileges	Administrator	List of authorized users with access privileges	This can be done later in the implementation phase, but should be completed before the start of the user acceptance testing.
4. Update user requirements specification for configured working practices	Process Owner User Quality Control and/or Quality Assurance	Updated user requirements specification	The user requirements used to select the system is generic and will not usually be specific to the application selected for implementation and validation. Ensure that data integrity requirements are updated to match system capability (see Appendix 3 on Data Integrity). Part of decommissioning also may include system decontamination, and if applicable, removal/ retirement of master data “object” from LMS or ELN.

Table 13.4: Project Phase (Prototyping and Specifying Software Configuration) (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
5. Perform requirements level risk assessment	Process Owner User	Requirements risk assessment	Input from the user requirements and the system configuration used to determine the highest risk requirements.
6. Write traceability matrix	Process Owner User	Traceability matrix	
7. Identify procedures to be written, updated or made historical	Process Owner System Owner	List of SOPs required for the system	From the traceability matrix, requirements that trace to procedures need to be identified and the procedures written.

Table 13.5: Project Phase (User Acceptance Testing and Validation Reporting)

User acceptance testing should verify that the user requirements can be met and that the system operates correctly. Verification activities typically occur on the production system. Where verification is split between test and production environment, there should be evidence to show equivalency between the two environments.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Finalize user procedures for all aspects of the system, e.g., use, instruments, administration	Process Owner Administrator	User SOPs User account Management SOP	Procedures should be followed during verification activities.
2. Establish instrument use records for all instrumentation in the system	Process Owner User	Instrument use and maintenance records	
3. Review supplier software testing document	Process Owner	Supplier testing of the application	See Appendix 11 on Supplier Documentation and Services. Determine extent of user acceptance testing to be performed.

Table 13.5: Project Phase (User Acceptance Testing and Validation Reporting) (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
4. Write user acceptance test documents based on intended use requirements and software configuration	Process Owner System Owner User Quality Control and/or Quality Assurance	Test plan Test scripts with procedures and acceptance criteria Updated user requirements specification and associated documents	Challenge access to application, configuration, and any remote data storage areas. It is likely that the URS and other associated documents will need to be updated, as requirements are refined during this phase of work.
5. Complete verification tests	Process Owner User IT Representative	Completed test scripts with documented evidence (both paper and electronic forms) Identification and resolution of test issues Deviations from test scripts with resolution of the issues	Tests should include intended use functions as well as non-functional tests and data storage. Capacity tests should be meaningful and based upon laboratory requirements. Testing should include verification of data integrity, audit trail function, and electronic signature use.
6. Write Validation Summary Report	Process Owner System Owner Quality Control and/or Quality Assurance	Validation summary report	Review of all validation activities and open issues prior to first use in production. Release of system for operational use.

Table 13.6: Operation Phase

The Operation Phase requires that change control, incident and problem management is effective and that periodic reviews are conducted according to the frequency determined by risk assessment and company procedures.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Place system into use	Process Owner	Change control request for placing system into operational use	Other alternative release mechanisms are acceptable.
2. Establish and ensure continued performance	Process Owner System Owner Supplier	Service level agreement with IT Software maintenance agreement Instrument service and maintenance agreement and calibration schedule	Instrument maintenance can be provided by a third party service agent.
3. Execute change management, incidents/problems	Process Owner System Owner Quality Control and/or Quality Assurance User	SOPs for managing changes, incidents and problems. Instrument use and maintenance records System change records Incident/problem records Corrective/preventative actions	Key to ensuring that the system remains in a validated state.
4. Perform Periodic Reviews	Process Owner System Owner Quality Control and/or Quality Assurance User	Periodic review report Action plans	Review last complete validation, change requests and any revalidation work, problems and incidents, user management records, security issues, looking for trends in performance. Confirm that data integrity measures are in place and work (see Appendix 3 on Data Integrity). Review IT support including backup and recovery, security, IT changes that could impact the system. Review maintenance, calibration, and service records. Review user training records especially after application upgrades and changes.

Table 13.7: Retirement Phase

At the end of the system life cycle, the data, procedures, and log books should be migrated or archived. Hardware components should be retired or reallocated to the new system.

Activity	Personnel	Deliverables/ Documentation	Comments
1. Collect information about the system: system components, data volumes, data owners, etc.	Process Owner Administrator	Current system configuration confirmed or reconciled List of data sets with owner	Business procedures and applicable regulations will determine which data must be retained.
2. Write Decommissioning (Retirement) Plan	Process Owner System Owner Quality Control and/or Quality Assurance Supplier	Retirement/migration plan	Specifies tasks and documented evidence for retirement of procedures, instrument records, instruments, computer hardware, application software, and regulated data. Defines the roles and responsibilities of those involved in the process.
3. Cease operational use of system	Process Owner System Owner Quality Control and/or Quality Assurance	Set a date when operational use of the system ceases	Retirement of the system should be performed when there is no operational use of the system.
4. Remove systems from the laboratory or reassign to replacement system	Process Owner Quality Control and/or Quality Assurance	Removal or reassignment of instruments Maintenance/use records	Update new system configuration or remove from inventory and asset lists. Cancel maintenance or calibration schedule, if appropriate.
5. Identify records to migrate or retire	Process Owner System Owner Quality Control and/or Quality Assurance	Data Migration Plan	Consider migrating data, to new system, or a read only version of existing system.
6. Execute work	Process Owner System Owner Quality Control and/or Quality Assurance	Verification Documents Data Migration Summary	If data are migrated to a new system, records of the migration need to be generated to demonstrate that the records have not changed content or meaning.

Table 13.7: Retirement Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
7. Write Decommissioning report	Process Owner System Owner Quality Control and/or Quality Assurance	Retirement report	Reviews activities performed and lists documented evidence collected.
8. Archive system documents	Process Owner System Owner User	Remove/retire SOPs, manuals and logbooks	Prevents use of retired materials.
9. If retired system is kept for data access, perform Periodic Review(s)	Process Owner System Owner Quality Control and/or Quality Assurance	Periodic review report	Review user management records and frequency of access. Verify continued ability to access records until retention period expires.

14 Appendix 7 – System Interfacing Considerations

This appendix highlights aspects that should be considered when interfacing a Laboratory Information Management System (LIMS) and/or Electronic Laboratory Notebook (ELN) with laboratory computerized systems in regulated organizations.

14.1 LIMS Overview

A LIMS is a configurable software system used for information and workflow management in laboratory operations. LIMS systems originated as data repositories. LIMS systems can now provide a sophisticated array of functions and features, including:

- Assay data management
- Data mining
- ELNs
- Interfaced laboratory instruments and equipment

Some functions may be considered as data management tools; given this level of complexity issues including data security and regulatory compliance should be considered. For further information, see Reflection Paper on Expectations on for Electronic Source Data [18].

14.2 ELN Overview

An ELN is a software program designed to replace paper laboratory notebooks. The ELN can provide advantages when compared to a paper notebook, including:

- Enabling data security
- Enabling users and regulators to easily and quickly search some or all entries (e.g., data mining functionality) in an accurate and repeatable manner
- Ensuring timely posting of experiments
- Facilitating workflows
- Improving readability

ELNs are used by scientists to capture experimental information and associated procedures. ELNs should assure that a record's authenticity, integrity, accuracy, traceability, readability, and security are maintained throughout the life cycle of the ELN.

Depending upon the use of the ELN, legal concerns may need to be addressed.

An ELN should be fit for intended use and should contain features such as configurable forms (to comply with the requirements of regulated analytical groups) to allow for the inclusion of structures, spectra, chromatograms, pictures, text, etc. Data within the system should be stored in a secure, structured, and searchable storage location such as a relational database. The system should enable data to be collected, stored, and retrieved through any combination of forms and/or ELN as appropriate.

The ELN should enable secure forms to be generated that accept laboratory data input via:

- PCs
- Laptops
- Mobile devices
- RFIDs
- Other electronic devices

The ELN should maintain a clear, secure link to electronic instruments such as laboratory balances, pH meters, etc. Data should be tabulated, checked, approved, stored, and archived to maintain compliance with regulatory expectations. Procedural controls should be established such that data entry is performed in the same way and the data can be interpreted uniformly throughout the organization.

14.3 Aspects to Consider

14.3.1 Scope of the System

The scope of the system should include the ELN/LIMS software, up to the point of data transmittal and/or receipt. Assessment should include verification activities that the data transmitted through these interfaces follow the quality and security parameters set forth by internal corporate policy. This approach focuses on how the ELN manages data, rather than on the infrastructure on which the ELN resides.

It is recommended that instrumentation is excluded from the scope of the ELN.

Dataflow and network diagrams can aid in the successful implementation of an ELN/LIMS and later assist in change management during operation. Establishing a scalable system scope may make future expansions or retraction of specific functions and/or parts of the system easier.

14.3.2 Global Impact Management

Organizations may implement a global LIMS, which helps to align processes across different sites and reduces IT cost. This approach requires appropriate Wide Area Network (WAN) infrastructure and data hubs for interfacing laboratory systems. The management of the global infrastructure and data should be assessed and harmonized where appropriate, and should be sufficiently scalable to support continued growth and expansion.

Additional controls should be considered, including data redundancy (e.g., business continuity and disaster recovery), especially if an ELN/LIMS is employed to support a 24 hour business model. Help desk and performance monitoring (although outside of the qualification scope) should be addressed with regard to international management strategies (e.g., how change management will be administered, actions to take, and people to contact if service is lost).

14.3.3 Data Transmissions across IT Infrastructure

This infrastructure supporting data transmittal should be maintained throughout the system life cycle. Key devices should be identified and device changes assessed for impact on the ELN/LIMS at the time of change.

For further information, see the ISPE GAMP Good Practice Guide: IT Infrastructure Control and Compliance [11].

14.3.4 Instrumentation Inputs

Instrumentation should be implemented according to the manufacturer's specifications at the design and functional levels. In highly integrated environments, an ELN/LIMS may function as the interface and control system for the instruments.

14.3.5 Records

Generated records to be retained, deleted, or archived should be defined. Review frequency of any defined records should be commensurate with their risk to data integrity, product quality, and patient safety.

Where "intermediate" records are created prior to the final record used for reporting purposes, the status and regulatory requirement for retaining the intermediate record should be determined. For example, if the original data was created on an instrument, and then that data was used in an electronic calculation that created new data, and both sets of data were entered into a new report file, there are potentially three records that should be considered.

ELNs/LIMSs may be global systems with local configuration choices that should be addressed and verified locally. This may impact regulatory filings and should be part of the risk management process.

14.3.6 Date and Time

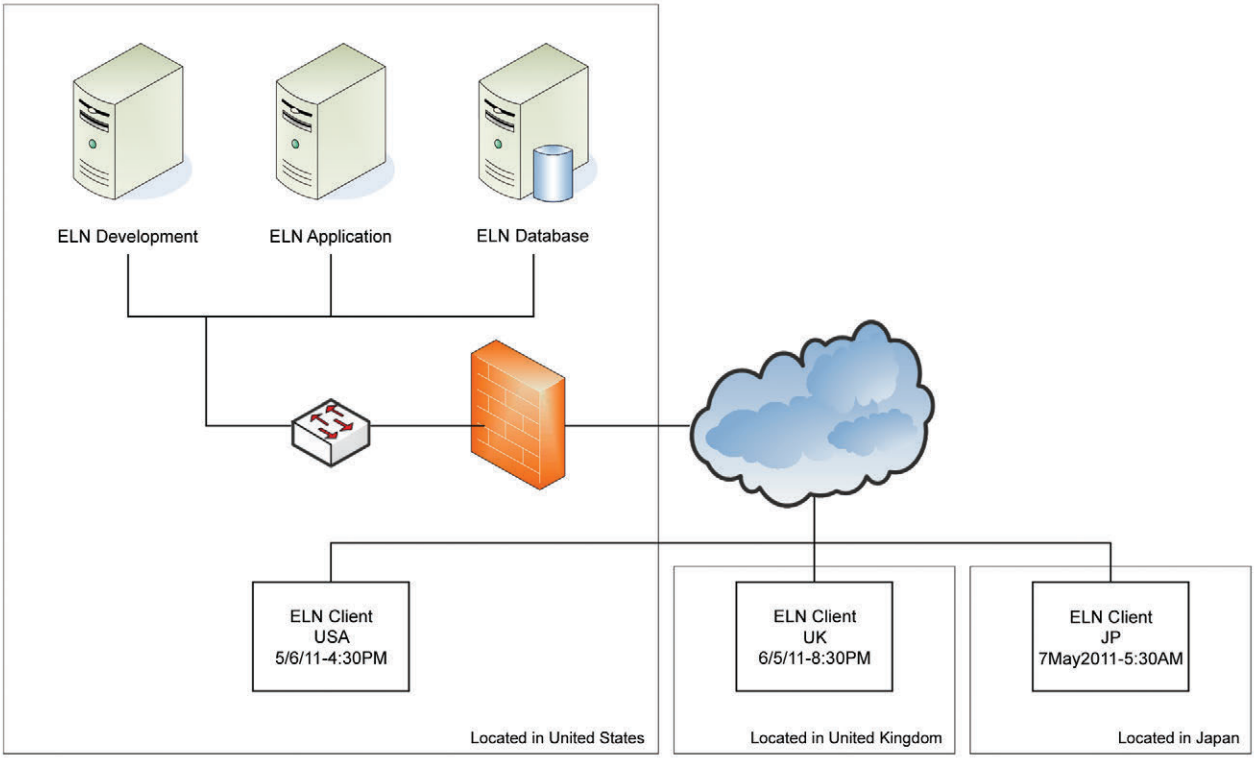
Date and time management should be set to Coordinated Universal Time (UTC), so servers, workstations, and other devices share a single reference. Figure 14.1 illustrates the complexity of time reporting in global applications. It is good practice to link the server host to a time service such as the NIST Internet Time Service [19]. Implement daylight savings time correction where applicable.

Time may be displayed in local setting configuration; however, audit trails should reflect UTC where possible.

Questions to consider include:

- Are the instruments and PCs dates and times equivalent to that recorded in the ELN/LIMS?
- How will date and time be documented (e.g., local date and time, or UTC) and what format is acceptable (e.g., 6May2011, 5/6/11, 6/5/11)?
- Does the e-signature date and time follow the defined standard?

Figure 14.1: What date and time is it?



14.3.7 Audit Trail

Links between audit trails for the software controlling instrumentation and the data entry into the ELN/LIMS should be evaluated to assure that the entries are identical. If there are differences in entries this could compromise data and an approach should be agreed upon and documented by key stakeholders including:

- Study director
- Quality Control and/or Quality Assurance
- Global system owners
- Legal experts
- Global process owner

Audit trails should capture documented evidence of all data runs executed, who they were executed by and when (time and date) they were executed. The audit trail also should reflect all data changes, including:

- What the changes are
- When the changes were made
- Who made the changes
- Why the change was made (e.g., change reason)

Corruption of the audit trail should be prevented and its integrity maintained. If data is allowed to be recalculated by inclusion or exclusion of specified data, this should be captured in the audit trail.

Procedural controls should be followed to assure reliability of data captured into the audit trail, e.g., periodic reviews of the audit trail entries should be performed at a regular, predetermined frequency.

14.3.8 Data Entry

The methods by which data is entered into the ELN/LIMS should be agreed upon to assure continuity of data and search ability after entry. Elements that should be agreed upon and documented should include:

- Data schema (i.e., how the data is organized)
- Data format types accepted and readable by ELN/LIMS
- Chemical and biological representations of compounds and biologics, such that interpretation of data is uniform (e.g., drawing rules and chiral flag representation)
- Experimental data entry methods (e.g., how to capture single point IC50 curves) overcoming business cultural and process differences
- The language (e.g., Japanese, English, Chinese) that in which the records should be written
- Methods of creating search templates or protocols for the ELN/LIMS (e.g., form development)
- Methods for rounding data during and after calculation
- The ELN/LIMS should incorporate procedural controls that are reasonably detailed including, if applicable:
    - Data that may have to be manually entered (e.g., some instruments may not possess the capability to be connected to the LIMS requiring manual entry, in the event of downtime manual entry may be required) or queried in the same manner regardless of location

14.3.9 Data Integrity

Experimental data integrity is typically maintained through peer review and may occur through the implementation of electronic controls. A data risk assessment should be performed including all data types, data management, and security methodologies, audit trails, etc., to assure that the data's integrity is maintained throughout its use and data transfer across interfaces. Data flow diagrams can be helpful in identifying which data is moved where and for assessing potential risks to the data's integrity. Data flow diagrams also can help in determining the impact of future changes to the system.

Data backup and recovery should be implemented to ensure data availability. Consideration should be given to off-site data storage locations. Disaster recovery management methodologies and business continuity plans to support ELN/LIMS should also be considered.

14.3.10 Data Archiving

A corporate data archiving policy should be implemented to reflect regulatory record retention compliance requirements (e.g., 21 CFR Parts 58.33(f), 195, 211.180, 11.1(b), 11.10(3), EPA Directive 2185 Section 8.4 [20, 21, 22, 23, 24, 25]) and internal corporate data utilization strategies. For further information on developing a corporate data archiving policy, see the ISPE GAMP Good Practice Guide: Electronic Data Archiving, Section 3 on creating and implementing an archive strategy [27].

14.3.11 Instrument Interfaces

Interfacing complex instruments that are application driven (e.g., HPLCs controlled by a CDS) involves more than just simple data transfer. It may involve creation of sequences in LIMS or ELN that are downloaded to the interfaced instrument or application.

Some interfaces require custom coding (such as writing parsing script code), whereas others are more template driven, making the interfacing process easier to implement. Further considerations include:

- Understanding where calculations applied to raw data are performed.
- Defining the specific attributes from the source application for upload to the ELN/LIMS and whether or not there are limitations, e.g., is there a limitation on the number of attributes of a peak in a chromatogram that can be uploaded.
- Determining the data flow, business rules and process flow (i.e., review and approval of results with the application of an electronic signature) so that the appropriate configuration parameters in both the source (i.e., CDS) and destination applications (ELN/LIMS) are well understood and defined.
- Verifying, with documentary evidence, that the required level of data precision is maintained during data transfer.
- Establishing the business continuity/system downtime procedures should the ELN/LIMS go down and where data still needs to be collected.
- Defining the data security measures based upon data storage (e.g., temporary local storage) and criticality.

14.3.12 Scientific Data Management Systems (SDMS)

The complexity of data storage and retrieval from multiple types of laboratory systems is ever increasing. The absence of a common storage solution leads to the requirement for well defined formal administration and maintenance processes.

The time and cost of maintaining these systems may be reduced with the use of a Scientific Data Management System (SDMS). Use of such systems can facilitate long-term storage, accessibility, and retrieval of scientific data by using an electronic/technology neutral format where the stored data is fully traceable to the source data.

Other advantages of using SDMSs include:

- The ability to exchange data with ELN, LIMSs, and other enterprise systems commonly used in the laboratory setting
- The ease of integration with existing IT infrastructure
- Providing a secure, compliant data repository

The validation lifecycle of an SDMS would follow GAMP® 5 [1].

14.4 ELN/LIMS Interface Verification Approach

Tables 14.1 to 14.4 provide a guideline for activities, which may be used when interfacing an ELN or LIMS with laboratory instruments and equipment in regulated organizations. These activities should be selected to meet the needs of the system in accordance with its intended use in the laboratory. Some of these activities may not be required. Activities may involve only simple checklists or forms.

Note: the tables in this appendix indicate typical roles which may be involved in each activity. The extent of the involvement of Quality Control (QC) and Quality Assurance (QA) depends upon the GxP impact and an organization's quality management processes and procedures.

Table 14.1: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify the scope of the system and which instrument interfaces will be used.	Process Owner System Owner IT Representative	Instrument manuals	Manuals required to determine the capability of each instrument to be interfaced to the ELN/ LIMS.
2. Identify initial technical requirements for interfaces	System Owner IT Representative Supplier	Technical documentation that identifies the instrument source (i.e., COM_DIRECT, COM_ FILE, FILE, FTP).	Different sources will allow for parsing measurement data in a particular way. This also will depend on the ELN/ LIMS. Requirements should include what the interface requirements are for a given instrument or class of instruments, including interface type and parsing scripts. Determine the interface type and whether or not parsing scripts are required.
3. Obtain resource and funding	Process Owner System Owner IT Representative	Project approval	Global implementations of applications may require compromises between different management/ business structures. This may take considerable effort to resolve.

Note: establishing verified IT infrastructure (e.g., virtual servers, physical servers, firewalls, switches, disc arrays) can reduce project implementation turnaround, assure data integrity and quality, and assure installed components that support data flow are working within manufacturer's recommended parameters (e.g., temperature, percentage relative humidity, power, backup, virus protection, and performance monitoring).

Table 14.2: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Develop requirements (URS, FS, and DS) documentation	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Requirements documentation	This is similar to other computerized systems as this detail will specify what is necessary for a successful installation and use of the ELN/LIMS. Assure intellectual property and internal requirements and all applicable regulatory requirements (e.g., 21 CFR Part 11, HIPPA, Annex 11 [26, 27, 17]) are included. In global applications, assure input and buy-in from all sites that will be using the application. Determine the data flow, process flow, and business rules that will apply to the use of the application and incorporate these into requirements.
2. Develop instrument interfacing requirements documentation	System Owner IT Representative Quality Control and/or Quality Assurance	Requirements documentation	The requirements can be an addendum to the overall ELN/ LIMS requirements documents or standalone requirements documents.
3. Perform risk assessment	Process Owner System Owner SME Quality Control and/or Quality Assurance	Risk assessment	To identify low, medium, and high risk requirements.
4. Configure the appropriate master data in ELN/LIMS	System Owner SME Quality Control and/or Quality Assurance	Configured master data	This includes writing/ associating the parsing script, if applicable.

Table 14.2: Project Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
5. Verify ELN/LIMS installation	System Owner SME Quality Control and/or Quality Assurance	Completed verification	Use supplier test protocols to assure the ELN/LIMS application is properly installed to enable required interfacing.
6. Develop internal procedures to identify daily data and system use	Process Owner System Owner SME Quality Control and/or Quality Assurance	Approved SOP documents	Ensure appropriate SOPs are created or revised to support the interface.
7. Verify ELN/LIMS instrument connectivity and qualify the interfaces	Process Owner System Owner SME Supplier	Completed protocol	This covers installation and operational verification.
8. Complete performance verification	Process Owner System Owner SME End User	Completed protocol	Verify using site-specific supplier performance verification documentation to qualify the use of the ELN/LIMS in regard to its operational and/or process requirements; assure testing satisfies all high and potentially medium risk requirements.
9. Create Validation report	Process Owner System Owner Quality Control and/or Quality Assurance	Validation report	Summarize results, assure all corrective actions have been completed, assure training of personnel has been completed, and then release the system for use.

Table 14.3: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Place the ELN/LIMS into operational use	System Owner	Change control request for placing system into operational use	
2. Implement change and configuration management and data maintenance procedures.	Process Owner System Owner Quality Control and/or Quality Assurance	Change and configuration management SOPs	Manage systems, instruments, infrastructure, and interfaces. Additional documentation covering typical problem resolutions can be helpful to improve system reliability.
3. Perform periodic reviews	Process Owner System Owner Quality Control and/or Quality Assurance	Periodic review report Action plans	The periodic review for an interfaced instrument to ELN/LIMS may be incorporated in the ELN/ LIMS periodic review or the instrument periodic review (if applicable) so that additional documentation for the interface does not need to be generated. Assessment of its function does not have to be a separate deliverable. Potentially, refine internal processes to increase productivity and reduce waste.

Table 14.4: Retirement Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify the scope and components to be decommissioned	System Owner IT Representative Quality Control and/or Quality Assurance	Identified components	
2. Create Decommissioning Plan	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Retirement plan	Identifies specific ELN's/ LIMS's instrumentation, code, component(s), and/ or interfaces that are to be retired; all system's supporting documentation is changed or retired; and specifies the identified equipment, procedures and data and the location to which the audit trail and data will be migrated.
3. Identify records to migrate or retire	Process Owner System Owner Quality Control and/or Quality Assurance	Migration plan	Includes raw data, instrument data, and instrument control data.
4. Migrate data and/or retire the system per plan	Process Owner System Owner Quality Control and/or Quality Assurance	Verification Documents Data Migration Summary	
5. Remove from inventory list	Process Owner Quality Control and/or Quality Assurance	Updated inventory list	Cancel maintenance or calibration service level agreement and address retirement/removal of ELN/LIMS code for the interface (if applicable).
6. Create Decommissioning report	Process Owner System Owner Quality Control and/or Quality Assurance	Retirement report	Details the activities performed during the retirement and/or migration of data from the system.
7. Remove supporting materials from the active inventory	Process Owner System Owner Quality Control and/or Quality Assurance	Remove/retire SOPs, logbooks, manuals, spare parts	To prevent the use of the retired system. Signage may be a helpful indicator to scientific personnel that this system is no longer available for use.

Table 14.4: Retirement Phase (continued)

Activity	Personnel	Deliverables/ Documentation	Comments
8. If the retired system is to be kept for data access only, perform periodic reviews	Process Owner System Owner Quality Control and/or Quality Assurance	Periodic review reports	Create reports detailing who accessed the system and with what frequency. When access to data is no longer required, retire remaining systems using the steps identified above.

15 Appendix 8 – Robotics Systems

15.1 Overview

Robotics systems can be used for many different purposes in a laboratory. The complexity of a robotics system varies from out of the box automation to highly customizable solutions interfaced to several hardware/software components. This appendix provides guidance on specifying and verifying the use of complex robotics systems in a regulated organization. If the configuration and architecture is for a single intended use as designed and specified by the supplier, the approach detailed in Appendix 5 for medium systems may be more appropriate.

15.2 Planning Considerations

When planning a robotics system, it is important to have a clear definition of the system scope, particularly when interfaced to several different components. The scope can be determined in conjunction with the development of user requirements, but should be detailed with the help of SMEs. SMEs may be internal to the organization or external personnel provided by suppliers.

Conducting an initial risk assessment during the concept phase is recommended. A detailed knowledge of robot mechanics is necessary to:

- Determine potential technical risks
- Perform an accurate impact assessment of each of those technical risks

This initial risk assessment can have a significant impact on supplier and product selection.

There are three basic design types of robotics systems:

1. Cartesian robot arm
2. Selective Compliance Articulated Robot Arm (SCARA) (aka “Four axis” SCARA robot)
3. Articulated robot arm

    - Cartesian robot arms are the simplest type of robotics system with a low cost, single purpose automation subsystem or dedicated equipment due to its restricted range of motion. This design is typically dedicated to a single purpose such as assay testing.
    - SCARA can move freely, but only in a single geometrical plane. This design provides high degree of rigidity with very fast motion and precise repeatability. They excel at high speed material handling tasks.
    - Articulated robot arms have more joints than SCARAs, including horizontal and vertical joints, resulting in increased freedom of movement and more flexibility, similar to a human hand and wrist.

Software may be created by an equipment supplier or by a sub-contracted supplier. (Sub-contracted services is defined here as those services that integrate components from different suppliers to create the final product.) Where an equipment supplier uses a sub-contractor, the equipment supplier should provide sufficient evidence that software engineering practices are employed by the sub-contractor. These practices should be monitored on a regular basis to assure continued conformance with established policies, standards and procedures.

Services supplied by a sub-contractor should have appropriate quality review by the equipment supplier to help mitigate associated risks.

Where a supplier is new to the regulated industry, the technology is new, or several implementations of a robot system will be purchased, an onsite audit is recommended.

Knowledge of previous customers may help to indicate a supplier's capabilities. Both the site of software development and the site of production should be investigated. Where assays and associated hardware/software is developed by separate organizations, both organizations should be investigated. For further information on the conduct of a Software Supplier Audit, see Appendix M2 of GAMP® 5 [1].

The scope of the robotics system should be clearly defined. Consideration should be given to whether the robotics system is intended to be incorporated into an automation subsystem or to be used as a dedicated single purpose system. The scope also should include any contracts with suppliers.

For a dedicated predefined set of activities, manufacturers typically complete design of the robotics system prior to purchase. Where a robotics system is intended to be integrated with another system, a configuration and/or design specifications of the interface should be included in the verification and operation.

The supplier should provide the specifications and limitations (range) of the robotics system. The limitations should be compared to the business use of the robotics system as part of design verification. Security requirements should be considered, e.g.:

- Data directories should be secure and access defined.
- Alarm and error handling requirements should be defined so that the system recognizes fault conditions and records or sends error messages, etc.
- Audit trail requirements should be defined to include those that are critical for data integrity, system use, diagnostics, and auditing.
- Defined records should be created, secured, and reviewed to maintain the integrity of test results.

In addition to functional requirements, it is important to address aspects such as:

- Graphic user interfaces (including navigation)
- Operation of the robotic system
- Data integrity
- Data output
- Audit trails
- Backup and recovery
- Utilities and special environments (e.g., humidity)
- Sample contamination and cross-contamination
- Configuration control
- Reports and file exports, including required file format
- Global time

Where a robot is not networked, the event times should be recorded by the controlling robot. Access to the system clock should be restricted to help assure validity of time stamps. Where a robotics system is networked, the local server time should be used unless organizational policies have been established.

Data entry methods (e.g., manual versus interface transaction) should be determined. Any character restrictions required by the interface or receiving system, or specific language types or formats that are required transactionally, e.g., rounding of significant digits, should be defined. If the interface performs this function, it should be verified during the installation phase.

15.3 Risk Management Considerations

The initial risk assessment performed during the concept phase should be supplemented with more detailed functional risk assessments throughout the project phase, as requirements and solutions continue to be clarified.

Risk assessments should consider the intended use and the associated functionality needed to fulfill the intended use of the robotics system, e.g.:

- How would the loss of software configuration impact system performance?
- How would the configuration be restored?

If the robot is deemed low risk, basic calibration should be verified. If the robot is medium risk, e.g., temperature control, the calibration throughout the operating range should be verified.

Items to consider during the risk assessment include:

- Accuracy required for intended use
- Technological constraints
- Technical risks
- Data path (data integrity concerns)
- Environmental conditions, e.g., temperature
- Individual components of the robotics system need to be assessed separately (e.g., pipetting mechanism, plate holder, additional devices).
- Analytical method layered on the robotics system
- System complexity and novelty, user experience
- Impact to production schedule
- Lack of availability of robot
- Cross contamination if different sample types
- Mechanical components
- Accuracy

- New technology
- Product impact
- Patient impact
- Criticality of instrument functions and/or interface(s)

15.4 Verification Activities for Robotics Systems

Tables 15.1 to 15.5 provide a guideline for activities, which may be used for robotics systems in regulated organizations. These activities should be selected to meet the needs of the robotics system in accordance with its intended use in the laboratory. Some of these activities may not be required. Activities may involve only simple checklists or forms.

Note: the tables in this appendix indicate typical roles which may be involved in each activity. The extent of the involvement of Quality Control (QC) and Quality Assurance (QA) depends upon the GxP impact and an organization's quality management processes and procedures.

Table 15.1: Concept Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Define the Scope of the system	Process Owner User	1. Business Requirements (robotics system use) 2. Description of Business Use 3. Interface(s) with other system(s) 4. Risk Assessment	Identify specifications/ limitations/use

Table 15.2: Project Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Define the high level system architecture	Supplier	Specifications: Hardware and Software Robot design	Supplier perspective URS/FRS
2. Create User Requirements	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	URS	URS includes data flow needs
3. Supplier Assessment	User Quality Control and/or Quality Assurance Supplier	Selection of Supplier Checklist, questionnaire, agenda Standards for hardware, and software development	Audit Quality System audit, team assembly ISO, IEC, Medical Device classification Class 1, 2, or 3. Software Risk classification A, B, or C.
4. Risk Assessment	Process Owner System Owner User Quality Control and/or Quality Assurance Supplier	Functional requirements Team participation with input into risk mitigation activities and review and approval of the risk assessment Provide information on supplier development and testing activities	Technical risks, materials used, and risks for laboratory computerized systems
5. Define Validation Approach	User Quality Control and/or Quality Assurance Supplier	Validation Plan or Updated Validation Plan of the interfaced system(s) Review of Supplier documentation. Qualification package available. Information on third party suppliers. Information of firmware, or other software contained within their product.	

After supplier and product selection, critical functions performed by the robotics system should be verified, based on the type of the system and risks associated with the intended use. The initial risk assessment, completed during the concept phase, should be updated to reflect the selected system. Specific consideration should be given to:

- Interfaces to other systems
- Possible risks related to the installation, configurations, and/or customizations of the robotics system

The basis for risk assessment is a detailed user requirements specification. Expertise of users should be obtained during the creation of user requirements. Development of the URS should consider:

- Will the robot produce a result that could impact manufacturing business processes, such as product recall or batch rejection?
- Could the results lead to delay of batch release or rejection of partial batches?
- Does the instrument produce or assist in a result that has a substantial effect on the business process? Is there another analytical technique that confirms the result (e.g., assaying both HPLC and biological potency)?
- Is the technology new to the industry or the organization?
- Does the technology mitigate risks due to human errors encountered when completing a manual assay?

These types of questions can assist in “process mapping” of fundamental business operations. This helps in defining strategies for focused testing and mitigation of higher risk business processes.

Interfaces to other systems, such as LIMS, should be defined, e.g.:

- Map the interface fields from input to output for verification of results and critical audit trails
- Determine if particular file formats are required for transfer of data within the interface
- Establish criteria for data input to assure the specified output

Metadata necessary to assure data integrity should be documented and verified. For example, an audit trail of sample storage temperatures, if critical to data integrity and quality assurance, should be retrievable. An audit trail of the movements of a robotics system during the dilution sequencing may be used for verification during system testing when comparing results to a manual process.

Movement of data should be considered when assuring data integrity, e.g.:

- Will the data be stored by the robotics system’s data system or will it be transferred to a server or a LIMS?
- How will this stored data be used?
- Where the robotics system records temperatures, will this data be needed in the reconstruction of a study?

Supplemental verification may include equipment configuration, security and access control, data integrity checks, and verification of archiving functionality (if available).

Depending on the nature of the robotics system, some of the activities described in this section of the Guide may be optional. For a dedicated predefined set of robotics system activities, the manufacturer should design the robotics system to do the majority of quality assurance in the factory, e.g., sample preparation into a robot (or another vessel), the robot is designed to perform calibration checks, etc. User verification activities should focus on interfaces to other laboratory computerized systems, such as ELN and LIMS. Interfaces should be appropriately specified and verified with the validated analytical method and associated procedures.

Verification should consider the:

- Backup/restore capabilities
- Ability to detect changes in configuration
- Correct performance of the required audit trails

The ability to export files in the required formats, while maintaining data integrity, should be confirmed, together with defined critical metadata, and regional regulatory requirements.

Table 15.3: Project Phase (Risk Management and Verification Activities)

Activity	Personnel	Deliverables/ Documentation	Comments
1. Review Business Process	Process Owner System Owner User Quality Control and/or Quality Assurance IT Representative	User requirements Process flow if architecture is complex.	Robotics system usage, robotics system type
2. Update Risk Assessment	Process Owner System Owner User Quality Control and/or Quality Assurance IT Representative	Risk Assessment	
3. Functional requirements	Process Owner Supplier IT Representative User	Configuration, functional and design specification Interface specifications Robot specifications for performing the necessary functions Additional software tools or templates for evaluation	Custom built robotics system
4. Verification	Supplier/User Quality Control and/or Quality Assurance IT Representative	Installation verification protocol Installation verification interface Operational verification and performance verification protocol (can be combined)	Supplier installation may include installation verification protocol. Supplier specifications detail import file to another instrument. Performance verification parallel with a manual process if replacing a manual process.
5. Summarize Implementation	User Quality Control and/or Quality Assurance	Validation Report	Summarize all changes and deviations, etc.

Table 15.4: Operation Phase

Activity	Personnel	Deliverables/ Documentation	Comments
1. Place into use	Process Owner System Owner	Equipment SOP – depending upon company policies and GxP Verify training Maintenance/use log	Documentation based on regulatory requirements.
2. Establish and ensure continued performance	Process Owner System Owner Supplier	Equipment SOP – depending upon company policies and GxP Maintenance/use log Maintenance contract Cleaning schedule Calibration schedule Contract for system upgrades, etc. Firmware or software upgrades	Calibration and maintenance may be conducted internally or by a third party supplier. Ensure spare parts are available Review technical and release notes
3. Execute change management, incidents/problems	Process Owner System Owner User Quality Control and/or Quality Assurance	Maintenance/use log Equipment relocation procedure Change control procedure Routine maintenance procedure	May need to re-establish acceptance criteria (e.g., moving non-portable equipment to new location).
4. Perform Periodic Reviews	Process Owner System Owner Quality Control and/or Quality Assurance	Periodic review report	Items to consider include the review of incidents, user access, security, audit trails, and trends in performance. Frequency should be determined by risk classification of the instrument as well as any changes made to the instrument.

Table 15.5: Retirement Phase

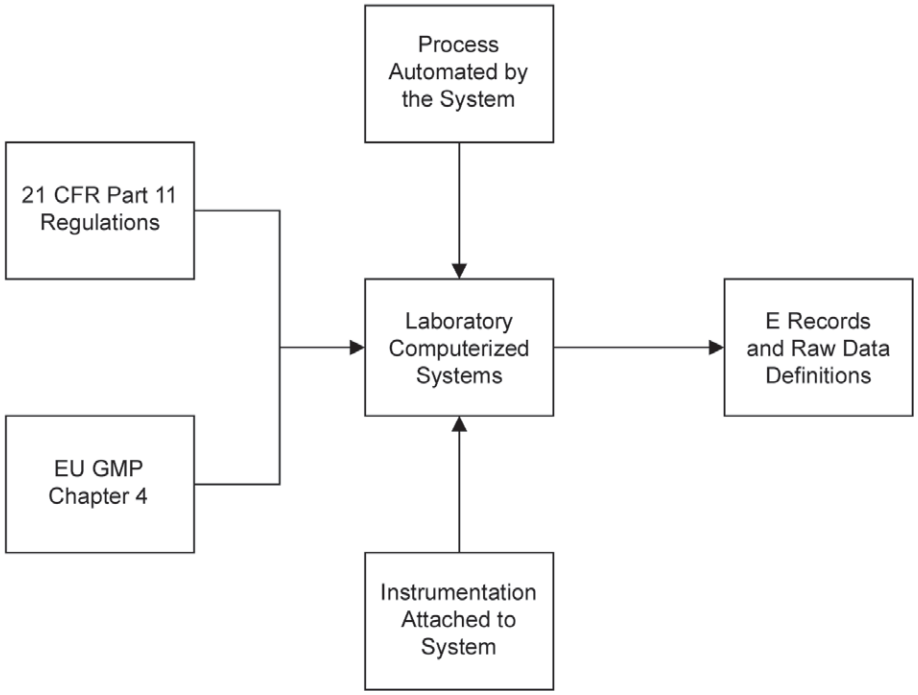
Activity	Personnel	Deliverables/ Documentation	Comments
1. Identify equipment/ components to retire	Process Owner System Owner IT Representative Quality Control and/or Quality Assurance	Identified components	
2. Create Decommissioning plan	Process Owner System Owner Quality Control and/or Quality Assurance	Retirement/migration plan	Define what will be done with the robotic system hardware and software. Define what will be done with any applicable data, e.g., migration or archive or deletion (if copied into a LIMS or ELN).
3. Remove robotic system components as per plan	Process Owner System Owner User	Disposal document	
4. Archive all electronic records	IT Representative End User Quality Control and/or Quality Assurance	Electronic record archiving report	Data diagrams created during the project phase aid in identification of records for archive.
5. Report of Retirement	Process Owner System Owner Quality Control and/or Quality Assurance	Retirement report	Summary of work performed under retirement/migration plan and discussion of any variances.

16 Appendix 9 – Defining Electronic Records and Raw Data

The purpose of this Appendix is to derive a common approach for complying with both the current FDA approach for 21 CFR Part 11 [26] and also the revised EU GMP Chapter 4 [28] on documentation for the requirement to define raw data used to make quality decisions. After deriving common principles to meet both regulations; examples, based on the use of a Chromatography Data System (CDS) with both hybrid and electronic working practices, will describe the records and raw data that are generated.

The process described in this Appendix, shown in Figure 16.1, first considers the applicable regulations for a laboratory operation, then looks at the instrumentation attached to the computerized system, combined with the business process automated by the system to define the electronic records/signatures and/or raw data generated by the system.

Figure 16.1: Process Overview of Appendix 9



16.1 Regulatory Rationale for Defining Records and Raw Data

This section outlines the regulatory expectations for defining electronic records and raw data for computerized laboratory systems. The specific regulations applicable to the systems in question should be identified.

16.1.1 21 CFR Part 11 and Applicable Predicate Rule Regulations

The publication of the FDA's Guidance for Industry on Part 11 Scope and Application has clarified the need for regulated organization to identify the electronic records generated and used in regulated laboratory processes.

The key points from the FDA Guidance on Part 11 – Scope and Guidance [26] are:

1. Narrow Interpretation of Scope of 21 CFR Part 11

We understand that there is some confusion about the scope of Part 11. Some have understood the scope of Part 11 to be very broad. We believe that some of those broad interpretations could lead to unnecessary controls and costs and could discourage innovation and technological advances without providing added benefit to the public health. As a result, we want to clarify that the Agency intends to interpret the scope of Part 11 narrowly.

Under the narrow interpretation of the scope of Part 11, with respect to records required to be maintained under predicate rules or submitted to FDA, when persons choose to use records in electronic format in place of paper format, Part 11 would apply. On the other hand, when persons use computers to generate paper printouts of electronic records, and those paper records meet all the requirements of the applicable predicate rules and persons rely on the paper records to perform their regulated activities, FDA would generally not consider persons to be "using electronic records in lieu of paper records" under §§ 11.2(a) and 11.2(b). In these instances, the use of computer systems in the generation of paper records would not trigger Part 11.

2. Definition of Part 11 Records

Under this narrow interpretation, FDA considers Part 11 to be applicable to the following records or signatures in electronic format (Part 11 records or signatures):

Records that are required to be maintained under predicate rule requirements and that are maintained in electronic format in place of paper format. On the other hand, records (and any associated signatures) that are not required to be retained under predicate rules, but that are nonetheless maintained in electronic format, are not Part 11 records.

In some cases, actual business practices may dictate whether you are using electronic records instead of paper records under § 11.2(a). For example, if a record is required to be maintained under a predicate rule and a computer is used to generate a paper printout of the electronic records, but users nonetheless rely on the electronic record to perform regulated activities (e.g. result trending or test result retrieval), the Agency may consider the official record as an electronic record instead of the paper record. That is, the Agency may take actual business practices into account in determining whether Part 11 applies.

Accordingly, we recommend that you determine, based on predicate rules, whether specific records are Part 11 records. For each record, you should determine whether you plan to rely on the electronic record or paper record to perform regulated activities. We recommend that you document this decision (e.g., in a Standard Operating Procedure (SOP), or specification document).

Electronic signatures are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules. Part 11 signatures include electronic signatures that are used, for example, to document the fact that certain events or actions occurred in accordance with the predicate rule (e.g. approved, reviewed, and verified).

16.1.2 European Union GMP Chapter 4 (Documentation)

EU GMP Chapter 4 on Documentation [28] requires that all data used for making quality decisions is identified for both hybrid (electronic records and paper printouts that are signed manually) and homogeneous (fully electronic systems with electronic signatures) data.

Chapter 4 Principle:

In this section, the types of documents expected from a regulated company are discussed. These include records, which are defined as providing evidence to demonstrate compliance with instructions. This section states that:

"Records include the raw data which is used to generate other records. For electronic records, regulated users should define which data are to be used as raw data. At least, all data on which quality decisions are based should be defined as raw data."

Generation and Control of Documentation

4.1 All types of document should be defined and adhered to. The requirements apply equally to all forms of document media types. Complex systems need to be understood, well documented, validated, and adequate controls should be in place. ***Many documents (instructions and/or records) may exist in hybrid forms, i.e., some elements as electronic and others as paper based.*** *Relationships and control measures for master documents, official copies, data handling, and records need to be stated for both hybrid and homogenous systems. Appropriate controls for electronic documents such as templates, forms, and master documents should be implemented. Appropriate controls should be in place to ensure the integrity of the record throughout the retention period.*

16.1.3 Summary of Regulatory Requirements

The requirements of 21 CFR Part 11 [26] can be summarized as:

- Know and understand the business process in the laboratory, coupled with the applicable predicate rule requirements
- Define and document the electronic records and signatures that are generated during the course of regulated activities
- Identify and manage risks to regulated records and signatures

Similarly, EU GMP Chapter 4 [28] requirements can be summarized as:

- Among the regulated documents are records that are required as evidence of actions from instructions such as analytical procedures, protocols, and standard operating procedures.
- For hybrid and homogeneous systems, regulated users need to define the raw data used to make quality decisions.

The requirements to document electronic records/raw data for both electronic and hybrid systems for EU GMP Chapter 4 on Documentation [28] and 21 CFR Part 11 [26] regulations are similar, and a single approach will suffice to meet both sets of regulations.

16.2 Illustrative Example: Defining Raw Data/Electronic Records for a Chromatography Data System (CDS)

This is an illustrative example only, and it is intended to be neither prescriptive nor definitive.

This example uses a Chromatography Data System (CDS), but the principles can be adapted to any other laboratory computerized system. This example discusses a system that is used electronically.

1. Define the Intended Use

This is required to determine the nature of the work and the business process supported by the system. An example of the intended use can be "the chromatography data system is a networked product that supports the chromatographic analysis of GxP work in development and manufacturing quality control laboratories."

From this, it can be inferred that the CDS will contain electronic records/raw data used for making quality decisions and these records will be signed electronically as defined in the User Requirements Specification (URS) for the system. Paper will be incidental to the main electronic operation of the system.

Therefore, the CDS will need to comply with the requirements of 21 CFR Part 11 [26] and also as quality decisions are made using the system, the CDS needs to comply with the requirements of EU GMP Chapter 4 [28].

2. Define the System Architecture

This is important to understand if the records are held centrally or are dispersed throughout the system. In this example, the CDS system uses client-server architecture. There are two types of data acquisition used by the system.

1. Chromatographs with instrument control and data acquisition functionality. These instruments are directly controlled by the CDS and all raw data/electronic records including the audit trail will be contained within the central data store of the system.

2. Original Equipment Manufacturers (OEMs) chromatographs that have data acquisition from the detector via an A/D (analogue to digital converter) to a data server, but are controlled using the original data system, which is a standalone controller. Control of the chromatograph will remain with the Original Equipment Manufacturers (OEM) data system, but the software also will acquire chromatographic data, as this function cannot be disabled. However all quantification and reporting of results will be performed within the client server CDS.

As a result of this architecture, there will be two versions of chromatographic data for each run – one in the CDS and one in the OEM data system (as the OEM data system acquisition function cannot be disabled). In this situation, the primary records will be contained within client server system and the OEM copy will not be considered as part of the definition of the business process. Therefore, as in the other case above, the networked CDS will contain the regulated electronic records and signatures.

The OEM data systems will be used solely for instrument control and will not contain 21 CFR Part 11 [26] records. As they control the instrument directly, copies of the instrument method should be printed out at the start and end of any analysis to meet requirements of the predicate rule. The reason for this approach is that the instrument files are not standardized and cannot be imported into the new client server systems.

3. Understand the Processes

Which regulated processes are automated by the CDS? These can vary from development (e.g., analytical development, toxicokinetics, bioanalysis and drug metabolism, clinical trial material production, and stability) to manufacturing (process validation, in-process manufacture analysis and PAT, quality control, stability, and retained/ retention samples.

4. Define the Raw Data/Electronic Records

The electronic raw data and electronic records/signatures generated by and maintained within the CDS now need to be defined by the laboratory. The same system, even within the same organization, can generate different raw data and electronic records depending on how it is used and the regulations applicable to its use.

Commercial CDS software systems may have file based records or those stored and managed using a database. The example records mentioned here can be guidance only and laboratories need to understand their individual installations (note that this list does not include software configuration settings or user account management). Examples may include:

- Individual files or projects with authorized users and instruments allocated to each one

- Instrument control files with versions showing any modifications used during the analytical run
- Processing method for fitting baselines to each injection
- Sequence files showing the injection sequence of System Suitability Test (SST), samples, blanks, etc., and any weights or correction factors used to calculate the final result
- Chromatographic data files of all injections from a run including test injections, System Suitability Test (SST) injections, failed sequences, and successful injections
- Calibration curve used and any associated calculations
- Reports with electronic signatures
- Audit trail entries of operator actions that create, modify, and delete records and raw data

A data flow diagram is a useful tool to visually map the flow of records throughout the business process and system.

17 Appendix 10 – Security Management for Laboratory Computerized Systems

17.1 Introduction

Security management is the process that ensures the confidentiality, integrity, and availability of an organization's regulated systems, records, and processes.

Security measures should be implemented to ensure that only authorized individuals may access the system and the data, and that the data are accurate and available when needed. Data should be adequately protected against willful or accidental loss, damage, or unauthorized change. Security management includes physical, logical, technical, and procedural controls to ensure the confidentiality, integrity, and availability of the system and data.

For most laboratory computerized systems, a single global security procedure is sufficient to ensure system security as long as the needs of the individual system can be accommodated to ensure accountability and integrity of records.

Specific technical details will change due to the continual advancement of new technologies and the nature of hazards may change. The administration of data security must be reviewed and updated frequently to ensure against new security threats.

17.1.1 Verification of User Identity

The unique identity of each authorized user of a laboratory computerized system should be established. Most companies require new employees to provide proof of identity before employment can begin, and a company Identification Card (ID) is issued. If this is followed, possession of a company ID should be sufficient to establish identity. In the absence of such a policy, the laboratory might establish user identity through an official, government issued ID, (such as a passport or driver's license with a photograph). In that case, a photocopy of the document used to establish user identity may be maintained in a secure, confidential file, though concerns for the protection of Personally Identifiable Information (PII) must be addressed.

17.1.2 Physical Security

The laboratory computerized system and the system software should be located in a limited access area of the facility. For stand-alone systems, physical security may substitute for a lack of logical security.

17.1.3 Physical Media

Disks, tapes, and other media used to store electronic records should be clearly and accurately labeled and stored in areas with appropriate environmental and access controls. It is advisable that backup copies are made of application software obtained on physical media and both copies be similarly protected. It is recommended that portable electronic media be physically secured, and where possible, encrypted to protect data. Multiple copies of media are often maintained to ensure data can be restored and protect from loss or corruption of data. External suppliers may provide these services.

17.1.4 Logical Security

In addition to preventing unauthorized access or damage to the application or operating system, access controls should be enabled to prevent access to modify the system clock, operating system permissions, and application system files. Deletion of data should be prohibited for the user. If deletion is required for system administration tasks, the process should be defined, justified, and approved by management and the deletion documented. As stated within the EU GMP Annex 11 Computerized Systems [17], some methods for preventing unauthorized access to a system include: the use of keys, pass cards, personal codes with passwords, biometrics, and restricted access to computer equipment and data storage areas.

Requirements for account management and passwords are often the subject of company policies and/or procedures.

17.1.4.1 User Accounts

Users should be granted the minimum set of privileges necessary to perform their job. In order to be effective, user accounts should require unique combination of user name and password. The setup password for the BIOS should be protected. To prevent the introduction of malicious applications, the boot sequence should be set in a way that booting with external media (e.g., DVD, USB key) is not possible after system setup. If user accounts are available at the operating system or application level, the BIOS start-up password is not required. User accounts should be set up at both the operating system and the application levels, when possible. The security implications for systems using the operating system and associated risks documented and managed, especially if Single-Sign-On (SSO) security scheme is implemented.

17.1.4.2 User Names

Each user name must be unique. Using a standardized naming convention is beneficial. It is important that user names are not shared as it is necessary to identify the individuals performing the work.

17.1.4.3 Minimum Password Length

Longer passwords are more secure, but are also more difficult to remember. Imposing undue restrictions or complexity on password length will typically result in users writing down the password, and keeping it near the computer. This is compounded, as a laboratory analyst may be required to use multiple laboratory computerized systems with potentially different passwords. This can defeat the purpose of the password and results in decreased security. A typical compromise is to require passwords to be at least six characters in length, and include both alpha and numeric characters. In certain situations, the use of special characters may be added to bolster security.

17.1.4.4 Password Age

Passwords should be changed periodically based upon assessed security risks. When possible, the software should be configured to force the password to be changed at a preset password-aging period (typically 30, 45, 60, or 90 days) or when specific events require immediate change (e.g., where the system administrator sets the initial password or changes it on the behalf of the user, typically after account lockout occurs). The system should detect and prevent previously used passwords, such that passwords are not repetitive or cycled on a periodic basis (e.g., three passwords used in cyclic pattern).

Forcing passwords to be changed too frequently may result in some confusion in users' ability to remember their new password. In that situation, users might write down the new password, and leave them near the computer for convenience. A systematic approach that combines both the password complexity and the preset password-aging period should be implemented to meet the perceived level of risk. Password management applications are available to provide security and monitoring.

17.1.4.5 Account Lockout

Accounts should be locked out after a specified number of unsuccessful logon attempts. Where the system permits, three consecutive attempts is a commonly used limit. The number of attempts before lockout should be defined in company policy. If system permits notification of the administrator for unsuccessful logon attempts, it should be enabled. If the system has electronic records and does not have such a notification, this deficiency needs to be addressed within the security plan.

Depending on the work environment (and the software settings), the account might remain locked until the administrator resets it. Permitting additional access accounts without administrator intervention should be permitted only after risk considerations.

17.1.4.6 Control of User Accounts

A process should be established to ensure that appropriate levels of management approvals are obtained for the creation, modification, or inactivation of user accounts, and the levels of access granted. This is commonly accomplished by use of a controlled form. A list of current and historical users including their roles and access privileges should be available. The EU GMP Annex 11 Computerized Systems [17], states that the "creation, change, and cancellation of access authorizations should be recorded."

Shared user accounts must be avoided as it is necessary to uniquely identify the specific users and their actions.

17.1.4.7 Groups

Common operating systems and many applications allow the creation of groups of user accounts. Groups assign access privileges and users are simply placed into the appropriate group. This is a far easier way to manage security when large numbers of users are present. When used, the purpose of the groups should be defined so that it is clear who belongs in a given group.

17.1.4.8 Active Session Integrity

Unattended active computer sessions (e.g., application is running) provide an opportunity for unauthorized personnel to modify data, using the identity of the user who started the application. To mitigate this integrity risk, password protected screen savers or other mechanisms to prevent unauthorized access should be utilized.

17.1.5 System Clock

The system clock should be secured to prevent users or suppliers from making inadvertent or intentional changes. As with all controls, a risk-based approach needs to be applied. If a system does not allow this level of technical control, procedural controls may be necessary. Additionally, for systems that are accessed across international time zones, consideration must be given to how date and time stamp access across these time zones will be recorded in the system. Tools are available to synchronize the internal network's authoritative time source with a very precise external time source.

17.1.6 Operating System Folders and Files

Some systems require files to run the instrument to be in the same directory as the test results. This configuration should be avoided as it requires all users to have write access to the areas where test results are stored, compromising data integrity. Many stand-alone laboratory systems can not conform to this and procedural controls are necessary.

17.1.7 Audit Policies

Common commercial operating systems enable the auditing of many functions performed on a computer. They are present as tools for monitoring the use and attempted misuse of system and network resources, if properly configured.

Note: these audit capabilities were not necessarily designed or intended to comply with 21 CFR Part 11 [26] or other electronic record and signature requirements. For further information, see Appendix 3.

The system application should have audit trail functionality to ensure that all critical user activities are recorded.

Audit policies should be set with care since the corresponding records can grow in size and quickly become unmanageable. A common strategy is to audit by exception. For example, logon failures or unsuccessful access of a network resource can be audited. This way, the logs are small enough that personnel will regularly review them.

17.1.7.1 Audit Policies for the Application

If the supplier, as a part of the base application, provides audit policies for the application, these should be enabled.

If it is possible to audit individual elements of a record produced by a system, the data to be audited should be defined and reviewed in pre-defined periods.

System security policies should be re-assessed in the periodic review and changed based on attempted and real security breaches.

A security process aimed at the highest possible level of security, which takes account of risk tolerances, will provide the best assurance of system security, and ultimately, data integrity.

17.1.8 Hot Fixes/Patches and Virus Definitions

The proper application of hot fixes/patches and virus definitions is an important activity. If the laboratory computerized system is networked, security measures must be taken to protect this environment. It is generally accepted that virus definitions do not impact the configuration of the operating system or the application, thus virus definition updates are encouraged according to company policies. For the installation of hot fixes/patches of the operating system, an assessment should be in place, which defines the process based on the risk and impact of the system.

The vendor or support service provider should not be allowed to roll out application patches or upgrades automatically, remotely, or without first gaining authorization via the change control process.

For systems with PC control, consider restricting internet access to sites vendors require for upgrading software versions.

For guidance, see Appendix S4 of GAMP® 5 [1].

18 Appendix 11 – Supplier Documentation and Services

Although the responsibility for compliance with GxP regulations lies with the regulated organization, the supplier may have considerable involvement in the process. It is important for suppliers to have knowledge of the regulations governing the organizations to which they supply laboratory systems to be able to contribute fully in the implementation process.

GAMP® 5 [1] provides detailed guidance on supplier activities. This appendix provides further guidance for suppliers of laboratory computerized systems to meet the requirements and expectations of regulated organizations.

18.1 System Development by the Supplier

Typically a computerized laboratory system has been appropriately specified, developed, tested, and released by a supplier before a laboratory considers the purchase of such a system. Current EU GMP regulations for computerized systems (Annex 11 [17]) require that regulated users take all reasonable steps to ensure that systems were developed in accordance with a system of quality assurance.

18.2 Supplier Assessment

Before selecting a laboratory computerized system, regulated organizations should assess the quality system of the supplier, how the product has been developed, and/or how the service is to be delivered. Typically a key step in this assessment is the completion by the supplier of the regulated organization's audit questionnaire. For regulated organizations, this requires generating and maintaining the questionnaire and for suppliers the need to complete a multitude of different questionnaires. The supplier may be asked to complete different questionnaires from different organizations as well as several questionnaires from different sites of the same organization at considerable cost.

The purpose of this section is to develop a set of standard criteria that will satisfy the majority of organizations that request information from instrument suppliers about their quality systems and products. This is intended to satisfy due diligence for most computerized laboratory systems and save time for both suppliers and regulated companies.

The outcome will be that a supplier can send a potential customer this standard information to eliminate the need for multiple questionnaires.

18.2.1 Overview of Supplier's Quality Management System and Product Development

The quality system overview should only focus on the quality system and product development, test, release, and support and/or service, as applicable. The Quality Management System (QMS) applicable to the product being purchased should be described, for example:

- Provide a copy of the top level quality policy that outlines the organization's commitment to quality, including that of the senior management of the organization.
- Describe the basis of the organization's quality system with reference to any applicable standards, such as ISO 9001 [16], ISO 9003 [29] and TickIT [30].
- If the QMS is formally certified, state by whom and enclose a copy of the current certificate in the overview document.
- List the main QMS procedures for the product or service under consideration with a brief note explaining their purpose and/or objectives.

The following additional information is suggested for product(s) under consideration:

- Product history such as time on the market, frequency of updates, current number of users, etc. This enables characterization of the maturity and scale of product deployment.
- Intended environment of product (e.g., GxP regulated laboratory, 21 CFR Part 11 [26] or EU GMP Annex 11 [17] compliance).
- Product development should describe how the system is specified, built and tested, and how it has followed the QMS procedures. Also include processes for capturing, classifying, and resolving errors found in testing.
- Product life cycle should explain how risk assessment for the quality, fitness for purpose, and data integrity of the instrument and associated software is incorporated into the product
- Product release processes should describe pre-release criteria reviewed.
- Product support processes and resources, and customer notification of problems should be addressed.

18.2.2 Specific Product Information and Documentation

There may be the need for additional information depending on the nature and complexity of the system:

A. Defining User Requirements and Documenting System Functionality. The user is responsible for defining the intended use of any laboratory computerized system used in a regulated laboratory; however, a supplier can help greatly in the process.

   For simple laboratory computerized systems, e.g., an analytical balance, the supplier's specification is often used as a basis for user specification and this is established practice for USP <1058> [6] group B instruments. However, it is important for users to know how supplier specifications for the analytical instrument portions of the system are established and how the testing has been carried out with sensible ranges of use.

   For medium systems, the users may need greater help from a supplier to document their instrument and software user requirements, as the supplier knows the system and its overall capabilities.

   For complex systems, the supplier may assist the customer in defining or configuring the system for an intended use, based on their knowledge of the system and the laboratory needs. A summary document from the supplier containing a list of the system functions would be extremely useful to users.

B. Technical compliance with the requirements of both 21 CFR Part 11 (Electronic Records; Electronic Signatures final rule) [26] and EU GMP Annex 11 (Computerized Systems) [17]. This document would explain how the software complies with the technical requirements of these regulations, as interpreted and understood by the supplier. This document could take the form of a white paper that explains how the product and the software is intended to be used and how it complies with the regulations or could divide the whole of each regulation into the responsibilities for compliance between the supplier and the customer. An alternative could be a simple presentation of the technical requirements of these regulations and how the system can be used to comply with them.

C. A summary of internal testing carried out on the system (e.g., functions tested). This can reduce the amount of testing performed by the regulated organization. This would allow the validation team to assess what, if any, additional testing should be carried out depending on a risk assessment and the extent of system configuration and or customization to meet laboratory business requirements.

D. Release of software hot fixes and service packs should be accompanied by adequate release notes explaining the rationale for and impact assessment of the change on the overall system. For example, does a change impact a single part of the software (e.g., class) or have major ramifications throughout the whole system?

The impact assessment provided by the supplier in the release notes can be used by regulated companies as an input into their own change control processes. For simple laboratory computerized systems, the impact assessment can be specific as the software is not configured and the impact assessment can be a direct input to the user's change control process. However, for medium systems, with varying extents of configuration by different users, the supplier impact assessment should be used together with the software configuration and the criticality of the process automated as the input to change control.

Release notes also should include advice on particular measures or safeguards that the regulated organization should consider to minimize the risk of change to their validated system in view of the impact of the change(s) on the product. This is essential when dealing with compulsory instrument firmware and system software upgrades. Suppliers may use different methods to keep their customers up to date with information about software hot fixes and service packs: letter, e-mail, web site, etc.

18.2.3 Supplier Professional Services

A number of professional services could be offered by a supplier to a regulated laboratory; these can include provision of more detailed documentation of the supplier's quality system (other than described above), services for installation of a new system, and system qualification. It is important for suppliers to realize that the regulated laboratory is responsible and accountable for the services offered by third parties including suppliers and consultants. To ensure that sufficient due diligence is performed before and after the activities take place, the laboratory should consider the following:

A. Regulated laboratories using supplier professional services should review documentation critically and approve it before execution of the services, when considering the professional services offered by the supplier for installation of the system components and release of the system.

   Areas for review include:

   - Scientific soundness of the proposed approach
   - How the instrument is tested using traceable materials and calibrated test equipment
   - Information from the supplier about which component(s) of the laboratory computerized system have the greatest impact on system quality and data integrity and hence should be subject to the greatest level of control.

B. Full range testing of the instrument by the supplier during development could allow standardization of protocols for all customer installations. Some areas to consider based upon activity include:

   Proper pre-execution and post-execution review and approval of qualification documents, both electronic and hybrid, by laboratory and quality personnel should be described. The process should include review and approval of both electronic and hybrid records.

   Test rationale: included in the testing document should be a discussion that justifies the testing undertaken.

   User requirements should be compared against supplier tests. Any requirements challenged during supplier test execution should be noted in the traceability matrix.

   Test documentation should be recorded clearly and legibly. Evaluation of the test result (e.g., passed/failed) should be clear and unambiguous to permit independent review.

   Test documentation should be collated (e.g., attachment numbers, file name, etc.) and recorded (either on paper or electronically). Test problems must be managed, documented, handled, and resolved for both manual and automated testing.

C. Proposed testing should have limits/range that match the laboratory's requirements. If not, either the document will need to be modified to match or the laboratory must undertake further work on their own.

   Approval of the complete document after testing by the suppliers' engineer with an explicit statement that the system testing has passed or failed. If testing has failed, a reason or justification should be included. In this case the supplier's engineer is acting as a tester on behalf of the customer.

   Evidence that the engineer performing the work is adequately trained should be left with the completed testing documents.

D. Modular versus holistic testing of modular instruments (e.g., HPLC): installation and verification should be performed. Installation and testing of the individual modules of the system (modular testing) followed by an integration test of the whole system (holistic testing) to demonstrate that the individual modules functions as a system.

E. Traceability of measurements to national or international standards: where one instrument is used to test another (e.g., digital thermometers, flow meters), each item should be calibrated to traceable standards which cover the range of use in the laboratory. Measurement uncertainties of the test instrument must be smaller than the acceptance criteria. Correction factors for modified original calibration results should be justified and properly verified for accuracy.

18.3 Supplier Good Practices

Supplier and customer relationships require mutual trust as trade secrets and proprietary information may be exchanged. Customers share their business needs and processes while suppliers share their products, documentation, and services information. Supplier business details may include development strategies and intimate details of their business operation. This sharing usually takes place only after a Non-Disclosure Agreement (NDA) or similar contract has been established to protect both parties.

It is important that the regulated organization ensures suppliers understand the environment in which their systems will be used and the requirements and expectations of regulated companies. With this understanding, suppliers can prepare various deliverables to assist the regulated companies with efficient implementation of their system. When supplier deliverables are used to support the suitability of a system for intended use, those deliverables should meet GxP documentation standards.

During initial contacts, suppliers have the opportunity to:

- Describe their products and services and demonstrate how they can improve customers' businesses/processes
- Explain their Quality Management System (QMS) and any quality standards they follow, e.g., IEEE, ISO, ICH, and how they meet relevant regulatory expectations (e.g., EU Annex 11 [17], 21 CFR Part 11 [26]).
- Describe the different levels or tiers of service available to customers, including deployment support, maintenance, calibration, hosting, and help desk
- Describe their process for providing system updates, patches, or bug fixes
- Define any consulting services provided to customers. This may be the time to discuss how they will support the use of their product and /or services, including installation/verification documentation.

This supplier information should give customers a sense of reliability and trust in the product or service and the supplier. Often laboratory computerized systems are not standalone systems, but are integrated in existing system landscapes. Suppliers should give supporting information about possible interactions with other systems and known limitations, especially dependencies on third party products (drivers, databases, operating system patches, etc.) to enable their system to be integrated with other systems.

Documentation that suppliers may make available to their customers includes:

- User manuals
- A system description including a high level overview of functionality, data flow, and data storage, if applicable.
- A statement of the ability of the system to support and comply with various regulatory expectations such as EU Annex 11 [17] or 21 CFR Part 11 [26].
- Overview of how the product can be configured by system administrators and system users.
- Hardware or software needed for the system (e.g., possibility to run on virtual hardware, license verifications like hardware dongles)
- Limitations of use of the system.
- Overview of system security procedures, including a description of the security model, roles, and permissions.
- Environmental requirements for system installation and information about environments not suitable for system operation.
- Procedures for system installation, including actual installation protocols or checklists.
- Information and an overview of the supplier's quality management system.
- Guidance on procedures for system verification, including actual protocols with predefined test cases. The protocols provided should include testing limits, detection limits, precision, etc.
- Information on procedures necessary for the calibration, management, and maintenance of the system.
- Information and process for customers to receive system patches, bug fixes, or new releases. This information should contain enough detail to enable the users of the system to determine the necessary activities, including the risk of acceptance. The supplier might include implementation procedures and actual test protocols along with their system updates.
- Information about any necessary periodic maintenance activities, including calibration procedures.

For installation and maintenance of more complex systems in regulated environments, the supplier should:

- Understand the change management requirements for supporting the system in the regulated environment.
- Have a process to notify and advised users of problems with the system.
- Provide a level of support appropriate to the contractual relationships and consistent with the expectations developed when the system was sold.
- Work in partnership with the regulated organization to support resolution of problems identified with the system.
- Provide a mechanism for logging, managing, and resolving customer complaints and escalation, if required.

19 Appendix 12 – References

1. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems*, International Society for Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, www.ispe.org.

2. International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, ICH Harmonised Tripartite Guideline, *Pharmaceutical Development – Q8(R2)*, August 2009, www.ich.org.

3. International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, ICH Harmonized Tripartite Guideline, *Quality Risk Management – Q9*, Step 4, 9 November 2005, www.ich.org.

4. International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use, ICH Harmonized Tripartite Guideline, *Pharmaceutical Quality System – Q10*, Step 4, 4 June 2008, www.ich.org.

5. ASTM Standard E2500, 2007, "Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment," ASTM International, West Conshohocken, PA, www.astm.org.

6. United States Pharmacopoeia General Chapter, <1058> Analytical Instrument Qualification (under development at time of publication).

7. ISPE Website, www.ispe.org.

8. 21 CFR Part 211.160(b)(4) – Current Good Manufacturing Practice for Finished Pharmaceuticals, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

9. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Calibration Management*, International Society for Pharmaceutical Engineering (ISPE), Second Edition, November 2010, www.ispe.org.

10. ISO 10012:2003 Measurement Management Systems – Requirements for Measuring Processes and Measurement Equipment, www.iso.org.

11. *ISPE GAMP® Good Practice Guide: IT Infrastructure Control and Compliance*, International Society for Pharmaceutical Engineering (ISPE), First Edition, August 2005, www.ispe.org.

12. PIC/S Good Practices for Computerized Systems in Regulated "GXP" Environment" (PI 011), www.picscheme.org.

13. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems*, International Society for Pharmaceutical Engineering (ISPE), Second Edition, under development at time of publication, www.ispe.org.

14. *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures*, International Society for Pharmaceutical Engineering (ISPE), First Edition, February 2005, www.ispe.org.

15. *ISPE GAMP® Good Practice Guide: Electronic Data Archiving*, International Society for Pharmaceutical Engineering (ISPE), First Edition, July 2007, www.ispe.org.

16. ISO 9001:2008 Quality Management Systems – Requirements, www.iso.org.

17. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Annex 11 – Computerized Systems, ec.europa.eu.

18. Reflection paper on Expectations for Electronic Source Data and Data Transcribed To Electronic Data Collection Tools in Clinical Trials, 2007, European Medicines Agency, www.ema.europa.eu/.

19. National Institute of Standards and Technology (NIST) Internet Time Service, www.nist.gov.

20. 21 CFR Part 58.33(f) – Good Laboratory Practice for Nonclinical Laboratory Studies, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

21. 21 CFR Part 195 – Good Laboratory Practice for Nonclinical Laboratory Studies, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

22. 21 CFR Part 211.180 – Current Good Manufacturing Practice for Finished Pharmaceuticals, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

23. 21 CFR Part 11.1(b) – Electronic Records; Electronic Signatures, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

24. 21 CFR Part 11.10(3) – Electronic Records; Electronic Signatures, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

25. EPA Directive 2185 – Good Automated Laboratory Practices, Section 8.4 LIMS Raw Data, U.S. Environmental Protection Agency (EPA), www.epa.gov.

26. 21 CFR Part 11 – Electronic Records; Electronic Signatures, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

27. Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104-191, 110 Stat. 1936, enacted 21 August 1996).

28. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation, ec.europa.eu.

29. ISO/IEC 90003:2004 Software Engineering – Guidelines for the Application of ISO 9001:2000 to Computer Software, www.iso.org.

30. The TickIT Guide Using ISO 9001:2000 for Software Quality Management System Construction, Certification and Continual Improvement, Issue 5.0, ISBN 0-580-36743-9, DISC TickIT Office, January 2001, www.tickit.org.

20 Appendix 13 – Glossary

20.1 Acronyms and Abbreviations

A/D	Analogue/Digital
ALS	Automatic Liquid Sampler
API	Active Pharmaceutical Ingredient
ASQ	American Society of Quality
ASTM	American Society for Testing and Materials
BCP	Business Continuity Plan
BP	Binary Pump
CAPA	Corrective and Preventive Action
CDS	Chromatography Data System
COP	Community of Practice
COTS	Commercial Off-the-Shelf
CFR	Code of Federal Regulations
DAD	Diode Array Detector
DG	Degasser
DS	Design Specification
ELN	Electronic Laboratory Notebook
EHS	Environmental, Health, and Safety
EU	European Union
FLD	Fluorescence Detector
FDA	Food and Drug Administration
FS	Functional Specification
FTIR	Fourier Transform Infrared Spectroscopy
GC	Gas Chromatography
GCP	Good Clinical Practice
GDP	Good Distribution Practice

GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GPG	Good Practice Guide
GxP	Aggregation of GCP, GMP, GLP, GDP – often used for everything of interest for the regulatory bodies.
HPLC	High Performance Liquid Chromatography
IEEE	Institute of Electrical and Electronics Engineers
ICH	International Conference on Harmonization
IT	Information Technology
LIMS	Laboratory Information Management System
MS	Mass Spectrometer
MSD	Mass Spectrophotometer Detector
MWD	Multi-Wavelength Detectors
NDA	Non-Disclosure Agreement
NIR	Near Infrared
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PM	Preventive Maintenance
OEM	Original Equipment Manufacturer
PC	Personal Computer
QA	Quality Assurance
QbD	Quality by Design
QMS	Quality Management System
QRM	Quality Risk Management
RFID	Radio-Frequency Identification
RI	Refractive Index
RTM	Requirements Traceability Matrix
RS	Requirements Specification

SCARA	Selective Compliance Articulated Robot Arm
SDMS	Scientific Data Management System
SIG	Special Interest Group
SLA	Service Level Agreement
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SST	System Suitability Test
TCC	Thermostatted Column Compartment
TWP	Thermostatted Well Plate
URS	User Requirements Specification
USP	United States Pharmacopeia
UTC	Coordinated Universal Time
UV	Ultra Violet
VWD	Variable Wavelength Detector
WAN	Wide Area Network

20.2 Definitions

Acceptance Test (IEEE)

Testing conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system. See also Factory Acceptance Test (FAT), Site Acceptance Test (SAT).

Application Software (ISO)

Software or a program that is specific to the solution of an application problem.

Archive

The process by which electronic data and document stores are regularly copied and retained for long-term retention of the data. Archived data is generally removed from the on-line database.

Archivist/Archive Administrator

The owner of the archiving operations on a daily basis.

Assessment

Investigation of processes, systems or platforms by a subject matter expert or IT Quality.

Audit (ISO)

Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which agreed criteria are fulfilled.

Business Continuity Plan (BCP)

A document prepared to summarize the organization's business continuity activities. BCPs can address single or multiple systems.

Business Continuity Planning (ISPE) (1) (ISO) (2)

(1) The act of planning for the continued operation of the laboratory computerized system, laboratory, or site in the event of failures or disruptions. (2) A managed process for developing and maintaining cross-organizational plans to counteract interruptions to business activities.

Calibration (ISO 10012)

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.

Change Control (PDA)

A formal process by which qualified representatives from appropriate disciplines review proposed or actual changes to a computer system. The main objective is to document the changes and ensure that the system is maintained in a state of control.

Component

An element within a system, such as a pump or a valve, on a piece of process equipment. Components can be critical or non-critical depending upon their potential impact on drug quality.

Computer System (IEEE)

A system containing one or more computers and associated software.

Computerized System

A broad range of systems including, but not limited to, automated manufacturing equipment, automated laboratory equipment, process control and process analytical, manufacturing execution, laboratory information management, manufacturing resource planning, clinical trials data management, vigilance and document management systems. The computerized system consists of the hardware, software, and network components, together with the controlled functions and associated documentation.

Configuration (IEEE)

The arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts.

Decontamination

A process that reduces contaminating substances to a defined acceptance level.

Detectability (ICH Q9)

The ability to discover or determine the existence, presence, or fact of a hazard.

Deviation (ICH Q7)

Departure from an approved instruction or established standard.

Disaster

(1) Any accidental, natural, or malicious event which threatens or disrupts normal operations, or services, for sufficient time to affect significantly, or to cause failure of, the company. (2) 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.

Disaster Recovery Plan

A plan to resume a specific essential operation, function, or process of an enterprise.

Design (IEEE)

The process of defining the architecture, components, interfaces, and other characteristics of a system or component.

Design Qualification

A documented review of the design, at an appropriate stage in a project, for conformance to operational and regulatory expectations.

Design Review (IEEE)

A process or meeting during which a system, hardware, or software design is presented to project personnel, managers, users, customers, or other interested parties for comment or approval. Types include critical design review, preliminary design review, system design review.

Firmware

Software (firmly) embedded in hardware components.

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 company 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 a company operates. These include but are not limited to (further descriptions provided in this Glossary):

- GMP
- GCP
- GLP
- GDP
- Good Quality Practice (GQP)
- Good Pharmacovigilance Practice
- Medical Device Regulations
- Prescription Drug Marketing Act (PDMA)

Harm (ICH Q9)

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

Hazard (ICH Q9)

The potential source of harm (ISO/IEC Guide 51).

Hybrid System/Record

One that uses both non-electronic (e.g., paper or microfiche) and digital/electronic output media. Similarly, a hybrid record is a record comprising at least two components stored on different media, typically electronic and paper. An example of a hybrid record would be an electronic record that is printed and approved on paper with a handwritten wet ink signature.

Hysteresis

The difference between the readings obtained when a given value of the measured variable is approached from opposite directions.

Incident

Operational event which is not part of standard operation.

Installation (ANSI)

The phase in the system lifecycle that includes assembly and testing of the hardware and software of a computerized system. Installation includes installing a new computer system, new software or hardware, or otherwise modifying the current system.

Installation Qualification (PDA)

Documented verification that a system is installed according to written and pre-approved specifications.

Instrument

Device or devices used to carry out a measurement.

Interface (ISO)

A shared boundary between two functional units, defined by functional characteristics, common physical interconnection characteristics, signal characteristics, and other characteristics, as appropriate. The concept involves the specification of the connection of two devices having different functions.

Migration

The transfer of digital information from one hardware/software configuration to another or from one generation of computer technology to a subsequent generation. The purpose of migration is to preserve the integrity of digital objects and to retain the ability for clients to retrieve, display, and otherwise use them in the face of constantly changing technology.

For convenience, migration can be sub-divided into the categories format migration (conversion), system migration, and media migration.

Operational Qualification (PDA)

Documented verification that a system operates according to written and pre-approved specifications throughout all specified operating ranges.

Periodic Review

A documented assessment of the documentation, records, and performance of computer systems to determine if it is still in a validated state and what actions, if any, are necessary to restore its validated state. The frequency of review is dependent upon systems complexity, criticality, and rate of change.

Performance Qualification (PDA)

Documented verification that a system is capable of performing or controlling the activities of the processes it is required to perform or control, according to written and pre-approved specifications, while operating in its specified operating environment.

Preventive Maintenance

Typically based on calendar time or run time. The intent is to perform the maintenance activity on a regular basis so as to ensure the equipment is operating within tolerances, minimizing wear and/or preventing failures.

Process Owner

The person ultimately responsible for the business process or processes being managed.

Quality Assurance/Control

An independent part of the organization responsible for assuring, or controlling, the quality and compliance with predicate rules of all applicable products and services of the organization.

Quality Management System (ISO)

Management system to direct and control an organization with regard to quality.

Quality Risk Management (ICH Q9)

A systematic process for the assessment, control, communication and review of risks to the quality of the drug (medicinal) product across the product lifecycle.

Quality System (ICH Q9)

The sum of all aspects of a system that implements quality policy and ensures that quality objectives are met.

Requirement (ISO)

Need or expectation that is stated, generally implied or obligatory.

Risk (ICH Q9)

The combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51).

Risk Assessment (ICH Q9)

A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.

Risk Control (ICH Q9)

Actions implementing risk management decisions (ISO Guide 73).

Risk Management (ICH Q9)

The systematic application of quality management policies, procedures, and practices to the tasks of assessing, controlling, communicating and reviewing risk.

Security (IEEE)

The protection of computer hardware and software form accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations.

Severity

Measure of the possible consequences of a hazard.

Specification (IEEE)

A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component, and often, the procedures for determining whether these provisions have been satisfied.

Subject Matter Expert

Those individuals with specific expertise in a particular area or field. Subject Matter Experts should take the lead role in the verification of computerized systems. Subject Matter Expert responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results.

Supplier

An organization or individual internal or external to the user associated with the supply and/or support of products or services at any phase throughout a systems life cycle.

System Life Cycle

The course of developmental changes through which a system passes from its conception to the termination of its use; e.g., the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system.

System Owner

The person ultimately responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system.

T**esting, Functional** (IEEE)

(1) Testing that ignores the internal mechanism or structure of a system or component and focuses on the outputs generated in response to selected inputs and execution conditions. (2) Testing conducted to evaluate the compliance of a system or component with specified functional requirements and corresponding predicted results. Syn: black-box testing, input/output driven testing. Contrast with testing, structural.

Testing, Structural (IEEE)

(1) Testing that takes into account the internal mechanism [structure] of a system or component. Types include branch testing, path testing, statement testing. (2) Testing to insure each program statement is made to execute during testing and that each program statement performs its intended function. Contrast with functional testing. Syn: white-box testing, glass-box testing, logic driven testing.

System Life Cycle

The course of developmental changes through which a system passes from its conception to the termination of its use; e.g., the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system.

User/End User

The pharmaceutical customer or user organization contracting a supplier to provide a product. In the context of this document it is, therefore, not intended to apply only to individuals who use the system, and is synonymous with customer.

Verification (ISO) (1) (ASTM) (2)

(1) Confirmation, through the provision of objective evidence that specified requirements have been fulfilled. (2) A systematic approach to verify that manufacturing systems, acting singly or in combination, are fit for intended use, have been properly installed, and are operating correctly. This is an umbrella term that encompasses all types of approaches to assuring systems are fit for use such as qualification, commissioning and qualification, verification, system validation, or other.

Validation (FDA)

Establishing documented evidence which provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes.

Virus

Generic term for all the various types of malicious code that has been designed to breach a company's security requirements.

Day In, Day Out

Turn your desktop into a digital library *anywhere* with ISPE Subscriptions

ISPE's new subscription service brings you unlimited online access to a custom set of ISPE Guidance Documents for your auditing, compliance, regulatory, engineering and quality needs.

Travel much? Your subscription travels with you anywhere, any time. Find, read, search, save and print the most current docs available. Enjoy one-click access to historical, related and referenced materials while you work. Download usage reports any time you need them. Add company branding. Get system training – on-site or web-based – for large groups.

Choose individual Documents or complete sets from any of these ISPE Series:

- Baseline® Guides
- ISPE Guides
- GAMP5® and GAMP Good Practice Guides
- ISPE Good Practice Guides
- Add related third party content from the world's leading standards authorities, including AAMI, ASTM, BSI, CLSI, DIN, IEC and others

In all, an efficient solution.

Go to www.ISPE.org/Subscriptions or call Techstreet today to start saving time and money with this essential tool.

ISPE Subscriptions are offered in partnership with the Techstreet business of Thomson Reuters, the world's leading source of intelligent information for business and professionals.

TECHSTREET®
1.734.780.8000

THOMSON REUTERS

Connecting a World of Pharmaceutical Knowledge

ISPE®

TRUST
17 YEARS
OF COMPLIANCE LEADERSHIP

Confidence means having a single, virtually audit-proof protocol for all your multi-vendor qualification requirements. And confidence is the reason why since 1995, labs in North America and Europe have continued to rank Agilent as the #1 choice for general compliance services. Want to improve your validation consistency, free up staff time, and reduce costs? We're ready to help. Visit: **www.agilent.com/chem/comply**

The Measure of Confidence

As voted by customers
five consecutive times since 1995

Agilent Technologies