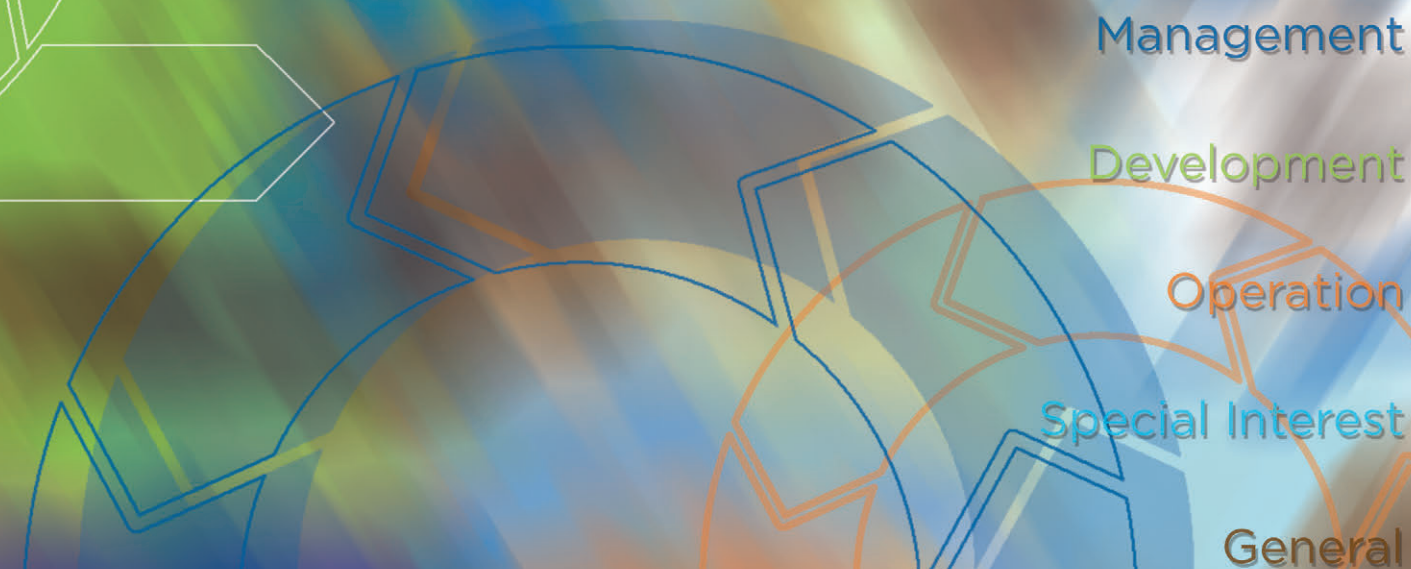




GAMP 5

A Risk-Based Approach to
Compliant GxP Computerized Systems
Second Edition



Critical Thinking

Enabling Innovation

Advancing Technology

AVA Documents
Document Sharing Hub



GAMP 5

A Risk-Based Approach to Compliant GxP Computerized Systems

Second Edition

Disclaimer:

The Guide is meant to assist life-sciences companies in managing GxP regulated systems. This Guide is solely created and owned by ISPE. It is not a regulation, standard or regulatory guideline document. 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.

© 2022 ISPE. All rights reserved.

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

All trademarks used are acknowledged.

ISBN 978-1-946964-57-1

Preface

The COVID-19 global pandemic underlined the essential role of innovation and technical advance in the protection of public health. This Second Edition of the *ISPE GAMP® 5 Guide* is intended to support such innovation and technical advance while safeguarding product quality and patient safety.

Such innovation is essential for life sciences industries in providing value to society while also controlling costs and reducing time to market.

Operating in a highly regulated industry may lead practitioners to apply prescriptive and rigid compliance-based approaches that are not commensurate with and not effective in managing any actual risk to the product and the patient.

This Guide facilitates the effective and efficient use of valuable resources by the application of appropriate and proportionate practices, encouraging innovative approaches to managing risk to patient safety, product quality, and data integrity, while supporting benefit to public health.

Acknowledgements

The Guide was produced by an international Task Team, under the leadership and direction of:

Chris Clark	TenTenTen Consulting Limited	United Kingdom
Heather Watson	GSK (retired)	United Kingdom
Sion Wyn	Conformity Ltd.	United Kingdom

The work was supported by the ISPE GAMP Community of Practice (CoP).

Chapter Leads

The following individuals took lead roles in the preparation of this document.

James Canterbury	Ernst and Young LLP	USA
Mark Cherry	AstraZeneca	United Kingdom
Frank Henrichmann	QFINITY	Germany
Paul Irving	Northern Life Sciences Ltd.	United Kingdom
Arthur D. Perez, PhD	Novartis (retired)	USA
Chris Reid	Integrity	United Kingdom
Michael L. Rutherford	Syneos Health	USA
Lorrie Vuolo-Schuessler	Syneos Health	USA
Eric J. Staib	Signant Health	USA
Thana Subramanian	Integrity	United Kingdom
Charlie Wakeham	Waters Corporation	Australia
Christopher H. White	National Resilience, Inc.	USA
Guy Wingate	GSK (retired)	United Kingdom

Contributors

The Leads thank the following individuals for their valuable contribution during the preparation of this Guide.

Sam Andrews	Novartis	United Kingdom
Karen Ashworth	Karen Ashworth Consulting Ltd.	United Kingdom
Carsten Bierans	Körber Pharma Software	Germany
Stephen R. Ferrell	CompliancePath (an Ideagen Company)	USA
James Gannon	PharmaLedger Association	Ireland
Senthil Gurumoorthi	Amazon	USA
Robert Hahnrahts	Bayer	Germany
James Henderson	Eli Lilly and Company	USA
Oliver Herrmann	QFINITY	Germany
David Samuel Holt	Factorytalk Co., Ltd.	Thailand
Torsten Isenberg	Körber Pharma Software	Germany
Paige Kane, PhD	Merck & Co., Inc.	USA
David Margetts	Factorytalk Co., Ltd.	Thailand
Andrew McDonagh	Emergn	United Kingdom
Elizabeth McLellan	Suvoda	USA
Sandy Meek	Parexel	United Kingdom
Khaled Moussally	Compliance Group Inc.	USA
Ray Murphy	Boston Scientific	Ireland
Mark E. Newton	Heartland QA	USA
Donal O'Brien	Dassault Systèmes	Ireland
Margrét Pétursdóttir	Alvotech	Iceland



Rajdeep Poddar	Novartis Healthcare Pvt. Ltd.	India
Edgar Röder	PricewaterhouseCoopers	Germany
Gregory Ruklic	GMR Consultants	USA
Judith S. Samardelis	GSK	USA
Levi Schenk	CSL Behring	USA
Tanya Sharma	Assurea, LLC	USA
Ken Shitamoto	Gilead	USA
Brandi M. Stockton	Signant Health	USA
Tomos Gwyn Williams	Manchester Imaging	United Kingdom
Christian Wölbeling	Körber Pharma Software	Germany

Regulatory Input and Review

The Core Team wish to thank the following individuals for their review and valuable comments on this Guide:

Kevin Bailey	MHRA	United Kingdom
Eric Dong	FDA	USA
Arno Terhechte, PhD	Bezirksregierung Münster	Germany
Seneca D. Toms	FDA	USA

Special Thanks

The Leads would like to thank ISPE for technical writing and editing support by Jeanne Perez (ISPE Guidance Documents Technical Editor) and production support by Lynda Goldbach (ISPE Publications Manager).

The Team Leads would like to express their grateful thanks to the many individuals and companies from around the world who reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

Company affiliations are as of the final draft of the Guide.



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

www.ISPE.org

AVA Documents
Document Sharing Hub

Table of Contents

1	Introduction	9
1.1	Rationale for GAMP 5 Second Edition	9
1.2	New and Revised Material	11
1.3	Purpose.....	11
1.4	Scope.....	12
1.5	Business Benefits	13
1.6	Structure	14
2	Key Concepts	17
2.1	Overview	17
2.2	Key Terms	19
3	Life Cycle Approach	23
3.1	Computerized System Life Cycle.....	23
3.2	Specification and Verification	25
3.3	Computerized System Validation Framework	26
3.4	Critical Thinking Through the Life Cycle	26
4	Life Cycle Phases.....	29
4.1	Concept.....	29
4.2	Project.....	29
4.3	Operation	40
4.4	Retirement	47
5	Quality Risk Management	49
5.1	Overview	49
5.2	Science-Based Quality Risk Management.....	50
5.3	Quality Risk Management Process.....	51
6	Regulated Company Activities.....	55
6.1	Governance for Achieving Compliance.....	55
6.2	System-Specific Activities	59
7	Supplier Activities.....	69
7.1	Supplier Products, Applications, and Services.....	69
7.2	Supplier Good Practices	70
7.3	Quality Management System.....	71
7.4	Requirements.....	72
7.5	Supplier Quality Planning.....	73
7.6	Sub-Supplier Assessments	73
7.7	Specifications.....	73
7.8	Design Reviews	74
7.9	Software Production/Configuration	74
7.10	Testing.....	75
7.11	Commercial Release.....	75
7.12	User Documentation and Training	75
7.13	System Support and Maintenance During Operation	76
7.14	System Replacement and Retirement	76

8	Efficiency Improvements	77
8.1	Establishing Verifiable and Objective User Requirements.....	77
8.2	Making Risk-Based Decisions	78
8.3	Leveraging Supplier Input.....	79
8.4	Leveraging Existing Information.....	79
8.5	Using Efficient Testing Practices.....	80
8.6	Employing a Well-Managed Handover Process	82
8.7	Managing Changes Efficiently	82
8.8	Anticipating Data Archiving and Migration Needs	84
8.9	Using Tools and Automation	84

Management Appendices

9	Appendix M1 – Validation Planning	85
10	Appendix M2 – Supplier Assessment	93
11	Appendix M3 – Science-Based Quality Risk Management.....	107
12	Appendix M4 – Categories of Software and Hardware	127
13	Appendix M5 – Design Review and Traceability	135
14	Appendix M6 – Supplier Quality Planning.....	141
15	Appendix M7 – Validation Reporting	145
16	Appendix M8 – Project Change and Configuration Management	149
17	Appendix M9 – Documentation and Information Management.....	153
18	Appendix M10 – System Retirement	157
19	Appendix M11 – IT Infrastructure.....	163
20	Appendix M12 – Critical Thinking	171

Development Appendices

21	Appendix D1 – Specifying Requirements	183
22	Appendix D2 (Retired)	197
23	Appendix D3 – Configuration and Design	199
24	Appendix D4 – Management, Development, and Review of Software	207
25	Appendix D5 – Testing of Computerized Systems.....	213

26 Appendix D6 – System Descriptions	235
27 Appendix D7 – Data Migration	239
28 Appendix D8 – Agile Software Development	245
29 Appendix D9 – Software Tools.....	253
30 Appendix D10 – Distributed Ledger Systems (Blockchain).....	257
31 Appendix D11 – Artificial Intelligence and Machine Learning (AI/ML)	269

Operation Appendices

32 Appendix O – Introduction to Operation Appendices	281
33 Appendix O1 – Handover	283
34 Appendix O2 – Establishing and Managing Support Services	287
35 Appendix O3 – System Monitoring	291
36 Appendix O4 – Incident Management and Problem Management.....	295
37 Appendix O5 – Corrective and Preventive Action.....	299
38 Appendix O6 – Operational Change and Configuration Management	303
39 Appendix O7 (Retired)	311
40 Appendix O8 – Periodic Review	313
41 Appendix O9 – Backup and Restore	319
42 Appendix O10 – Business Continuity Management	325
43 Appendix O11 – Security Management.....	331
44 Appendix O12 – System Administration	337
45 Appendix O13 – Archiving and Retrieval	341

Special Interest Topics Appendices

46 Appendix S1 – Alignment with ASTM E2500	347
47 Appendix S2 – Electronic Production Records.....	351
48 Appendix S3 – End User Applications Including Spreadsheets.....	361

49 Appendix S4 – Patch and Update Management..... 371

50 Appendix S5 (Retired) 375

51 Appendix S6 – Organizational Change..... 377

General Appendices

52 Appendix G1 – References 383

53 Appendix G2 – Glossary 389

53.1 Acronyms and Abbreviations 389

53.2 Definitions 392

1 Introduction

GAMP guidance aims to safeguard patient safety, product quality, and data integrity in the use of GxP computerized systems. It aims to achieve computerized systems that are fit for intended use and meet current regulatory requirements by building upon existing industry good practice in an efficient and effective manner.

GAMP provides practical guidance that:

- Facilitates the interpretation of regulatory requirements
- Establishes a common language and terminology
- Promotes a system life cycle approach based on good practice
- Clarifies roles and responsibilities

It is not a prescriptive method or a standard, but rather provides pragmatic guidance, approaches, and tools for the practitioner.

When applied with expertise and good judgment, this Guide offers a robust, cost-effective approach.

The approach described in this document is designed to be compatible with a wide range of other models, methods, and schemes including:

- Quality systems standards and certification schemes, such as the ISO 9000 Series [1]
- ISO 14971 [2]: Medical devices – Application of risk management to medical devices
- Schemes for assessing and improving organization capability and maturity, such as Capability Maturity Model Integration® (CMMI) [3]
- Software process models such as ISO 12207 [4]
- Iterative, and incremental (Agile) software development methods and models
- Approaches to IT service management, such as ITIL [5]

Where possible, terminology is harmonized with standard international sources such as ICH [6] and ISO [7].

This Guide aims to be fully compatible with the approach described in the ASTM E2500 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment [8].

GAMP is an ISPE Community of Practice. For further information see www.ispe.org.

1.1 Rationale for GAMP 5 Second Edition

This Second Edition Guide aims to protect patient safety, product quality, and data integrity by facilitating and encouraging the achievement of computerized systems that are effective, reliable, and of high quality.

While the overall approach, framework, and key concepts remain unchanged, technical content of the Guide has been updated to reflect the increased importance of IT service providers including cloud service providers, evolving approaches to software development including incremental and iterative models and methods, and increased use of software tools and automation to achieve greater control, higher quality, and lower risks throughout the life cycle.

Associated with this is the reinforcement of the message that the GAMP specification and verification approach is not inherently linear but also fully supports iterative and incremental (Agile) methods.

Guidance on the application of new and developing technological areas such as Artificial Intelligence and Machine Learning (AI/ML), blockchain, cloud computing, and Open-Source Software (OSS) has been included or updated.

The importance of critical thinking and the application of patient-centric, risk-based approaches (aimed at quality and safety) versus primarily compliance-driven approaches is further underlined. Concepts of computerized systems assurance as discussed as part of the US FDA Center for Devices and Radiological Health (CDRH) Case for Quality program [9] are also explored and applied.

Links and references to GAMP guidance on the topic area of record and data integrity have been added.

The following ISPE initiatives and topic areas are supported and links and synergies with them have been considered:

Knowledge Management – focusing on how organizations create, manage, and use knowledge throughout the life cycle of a product, enabling organizations to better manage their knowledge as a key asset, in turn improving the effectiveness of the pharmaceutical quality system, and providing operational benefits. [10]

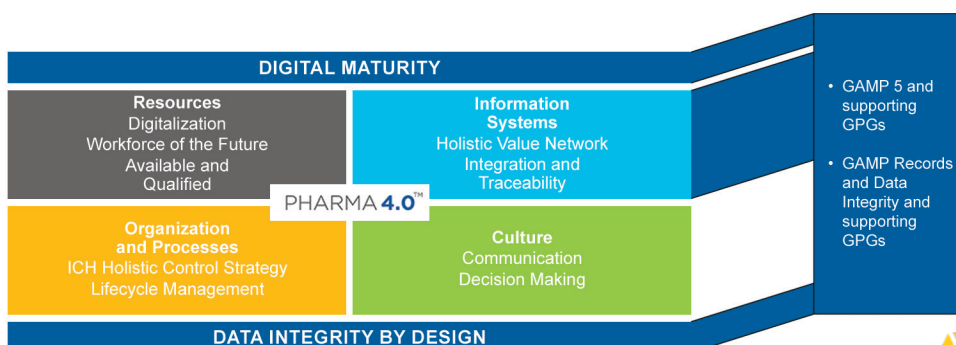
APQ (Advancing Pharmaceutical Quality) – building industry-for-industry tools and programs to help companies assess and improve their quality operations. [11]

Pharma 4.0™ – providing guidance, aligned with the regulatory requirements specific to the pharmaceutical industry, to accelerate Pharma 4.0 transformations. Also known as the Smart Factory, the objective of Pharma 4.0 is to enable organizations involved in the product life cycle to leverage the full potential of digitalization to provide faster innovations for the benefit of patients. [12]

Digital maturity and data integrity by design are enablers to an effective digitalization strategy and are underpinned by well-managed automation and information systems. GAMP guidance aims to ensure that GxP computerized systems are fit for intended use, and that GxP electronic records and data are managed throughout the data life cycle in order to ensure data integrity. See Figure 1.1.

GAMP guidance adopts a patient-centric risk-based approach that enables innovation while demonstrating compliance with regulatory requirements. Pharma 4.0 builds on best practices based on ISPE Guidelines that are enhanced by the digital transformational approach to real time data driven processes.

Figure 1.1: Pharma 4.0 [13]



1.2 New and Revised Material

New guidance has been included on the following topics:

- Appendix D8 – Agile
- Appendix D9 – Software Tools
- Appendix D10 – Distributed Ledger Systems (Blockchain)
- Appendix D11 – Artificial Intelligence and Machine Learning (AI/ML)
- Appendix M11 – IT Infrastructure
- Appendix M12 – Critical Thinking

Significantly updated guidance has been included on the following topics:

- Appendix D1 – Specifying Requirements
- Appendix S2 – Electronic Production Records

As a result of the above additions and revisions, the following guidance included in the previous version of this Guide have been removed:

- Appendix D2 – Functional Specifications
- Appendix O7 – Repair Activity
- Appendix S5 – Managing Quality within an Outsourced IS/IT Environment

The overall GAMP 5 framework, key concepts, system life cycle, specification and verification approach, and Quality Risk Management (QRM) process (aligned with ICH Q9 [14]) remains unchanged.

1.3 Purpose

The purpose of this Guide is to provide a cost-effective framework of good practice to ensure that computerized systems are effective and of high quality, fit for intended use, and compliant with applicable regulations. The framework aims to safeguard patient safety, product quality, and data integrity while also delivering business benefit. This Guide also provides suppliers to the life-science industry with guidance on the development and maintenance of systems by following good practice.

Patient safety is affected by the integrity of critical records, data, and decisions, as well as those aspects affecting physical attributes of the product. The phrase “patient safety, product quality, and data integrity” is used throughout this Guide to underline this point.

This Guide is intended for use by **regulated companies, suppliers, and regulators**. Suppliers include providers of software, hardware, equipment, system integration services, IT service providers, and IT support services, both internal and external to the regulated company.

The Guide has been designed for use by a wide range of disciplines and responsibilities, including:

- Management
- Quality Unit
- Research
- Development
- Manufacture
- Laboratory
- Engineering
- IT
- Support Staff
- All associated suppliers

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

1.4 Scope

This Guide applies to computerized systems used in regulated activities covered by:

- Good Manufacturing Practice (GMP) (pharmaceutical, including Active Pharmaceutical Ingredient (API), veterinary, and blood)
- Good Clinical Practice (GCP)
- Good Laboratory Practice (GLP)
- Good Distribution Practice (GDP)
- Good Pharmacovigilance Practices (GVP)
- Medical Device Regulations (where applicable and appropriate, e.g., for systems used as part of production or the quality system, and for some examples of Software as a Medical Device (SaMD¹))

These are collectively known as GxP regulations (see Chapter 2 for full definition).

This Guide provides an approach that is suitable for all types of computerized systems, focusing on those based on standard and configurable products, but equally applicable to custom (bespoke) applications.

¹ Medical devices have their own regulatory framework and standards (e.g., ISO 13485 [16], ISO 14971 [17], and IEC 62304 [18]), typically require individual approval, and are often subject to clinical trial evaluation after software verification. GxP computerized systems as discussed in this Guide usually support internal regulated company GxP business processes, whereas SaMD is typically a product in the hands of patients or health care providers.

The principles described can be applied to a wide range of computerized systems. Detailed application of these principles to specific system types (e.g., IT, infrastructure, process control systems, and analytical laboratory systems) is described in supporting *ISPE GAMP Good Practice Guides* [15].

Not all the activities defined in this Guide will apply to every system. The scalable approach, with application of critical thinking, enables regulated companies to select the appropriate system life cycle activities.

This Guide is also consistent with other regulatory demands such as Sarbanes-Oxley (SOX)² and those associated with data privacy. The use of this Guide, however, does not guarantee compliance with, or replace, these regulatory demands, which will define additional requirements where they are applicable.

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

1.4.1 Supplier Aspects

The computerized system life cycle described in this Guide for a regulated company should not be confused with the need for a defined approach or method for software development, which is the responsibility of the supplier.

This Guide defines activities and responsibilities expected of the supplier in the provision of products and services. These activities perform an important role in supporting regulated company activities. The supplier may be a third party or an internal group of the regulated company. Such internal groups should follow processes consistent with the regulated company Quality Management System (QMS).

This Guide uses various diagrams to represent the system life cycle. These diagrams often present relationships in a linear representation. This is not intended to constrain the choice of development methods and models. Suppliers should use the most appropriate methods and models, which may include iterative and incremental (Agile), evolutionary, exploratory, and prototyping techniques, or the use of DevOps approaches (see also Appendix D8).

Modern systems may have a complex supply chain involving multiple suppliers. This Guide aims to meet the needs of each group.

1.5 Business Benefits

Effective, reliable, and high-quality computerized systems assist in achieving the primary objectives of patient safety, product quality, and data integrity, but there are major business benefits in having a defined process that delivers systems 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. Adoption of the approaches described in this Guide will assist regulated companies in managing business risk as well as quality risks.

Specific benefits to both regulated companies 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 continual improvement

² The US Sarbanes-Oxley law [19], specifically Section 404, mandates control of computer systems that generate financial records. Many of the good practice principles and electronic records management controls are relevant to compliance with this law.

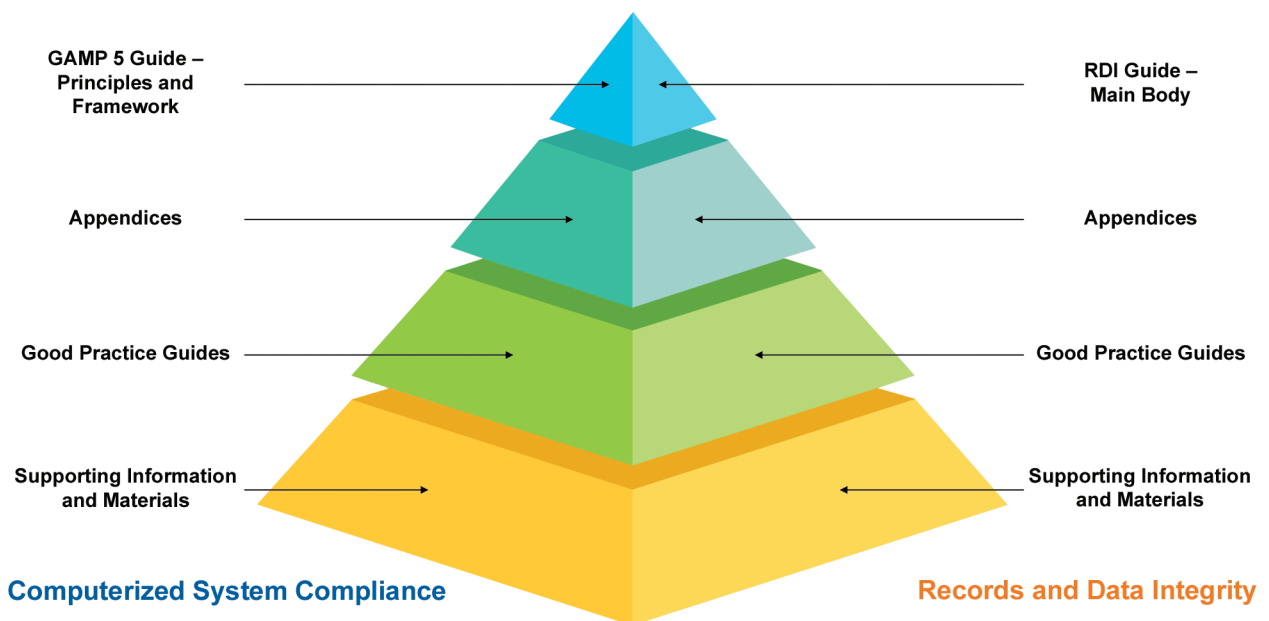
- Enabling of innovation and adoption of new technology
- Providing frameworks for user/supplier cooperation
- Assisting suppliers to produce required documentation
- Promotion of common system life cycle, language, and terminology
- Providing practical guidelines and examples
- Promoting pragmatic interpretation of regulations

1.6 Structure

1.6.1 Overview of GAMP Documentation Structure

This 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, as shown in Figure 1.2.

Figure 1.2: GAMP Documentation Structure [20]



This Guide comprises a main body and a set of supporting appendices.

The main body provides principles and a life cycle framework applicable to GxP regulated computerized systems.

Practical guidance on a wide range of topics is provided in the supporting appendices.

Separate *ISPE GAMP Good Practice Guides* [15] cover the application of these general principles and framework to specific types of systems and platforms. Other GAMP GPGs provide detailed approaches to specific activities and topics. For information about available *ISPE GAMP Good Practice Guides*, see www.ispe.org.

1.6.2 GAMP 5 Main Body Structure

The main body introduction covers the purpose, scope, benefits, and structure of this Guide. Subsequent sections of the main body cover the topics:

- Key concepts
- Life cycle approach
- Life cycle phases:
 - Concept
 - Project
 - Operation
 - Retirement
- QRM
- Regulated company activities:
 - Governance for achieving compliance
 - System-specific activities
- Supplier activities
- Efficiency improvements

The **key concepts**, described in Chapter 2, are the five concepts that underpin the rest of the document and should be applied using critical thinking.

The computerized system **life cycle** encompasses all activities from initial concept, understanding of the requirements, through development or purchase, release, and operational use, to system retirement. Chapter 3 describes these activities and how they are related.

Chapter 4 describes the **project life cycle phase** in more detail, including:

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

The key supporting processes of risk management, change and configuration management, design review, traceability, and document management are also introduced.

QRM is a systematic approach for the identification, assessment, control, communication, and review of risks to patient safety, product quality, and data integrity. It is an iterative process applied throughout the system life cycle. Chapter 5 describes this approach and how these activities should be based on good science and product and process understanding.

Ensuring compliance and fitness for purpose is the responsibility of the regulated company. Effective and consistent **regulated company activities** for individual systems require a defined organizational and governance framework, covering aspects such as policies, responsibilities, management, and continual improvement. Governance and system-specific regulated company activities are covered in Chapter 6.

While the responsibility for compliance lies with the regulated company, the supplier has a key role to play. An overview of typical **supplier activities** is given in Chapter 7.

This Guide provides a flexible framework for achieving compliant computerized systems that are fit for intended use, but the full benefits can be obtained only if the framework is applied effectively in the context of a particular organization. Chapter 8 covers key topics leading to **efficiency improvements**.

2 Key Concepts

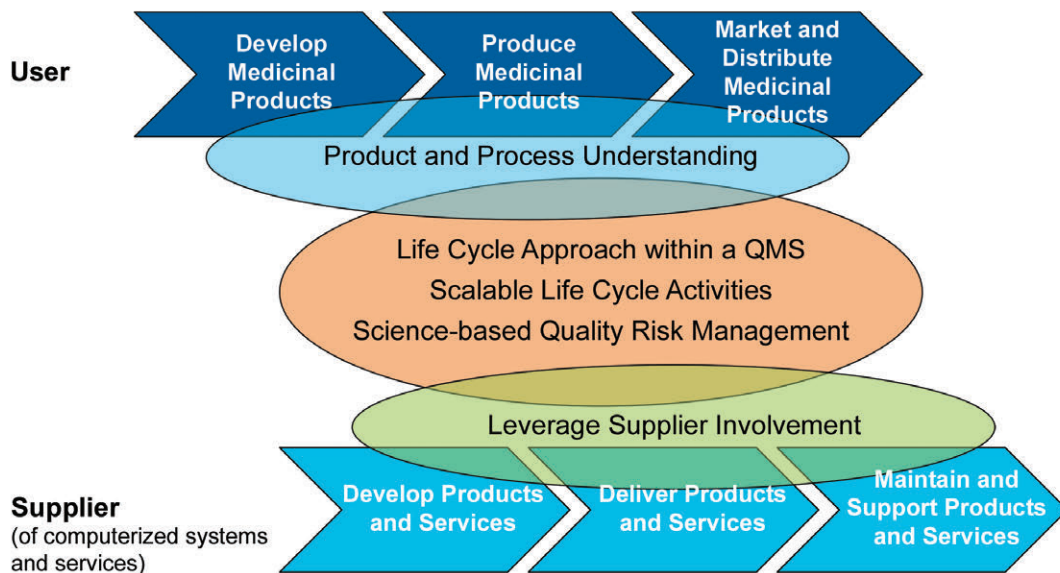
2.1 Overview

Five key concepts are applied throughout this Guide:

1. Product and process understanding
2. Life cycle approach within a QMS
3. Scalable life cycle activities
4. Science-based QRM
5. Leveraging supplier involvement

The relationship between these concepts is shown in Figure 2.1.

Figure 2.1: Key Concepts of this Guide [20]



2.1.1 Product and Process Understanding

An understanding of the supported process is fundamental to determining system requirements. 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. An understanding of the intended use of data within the process is also fundamental. Data integrity cannot be achieved without a complete understanding of the data flow.

As noted in ICH Q10 [21]:

“product and process knowledge should be managed from development through the commercial life of the product up to and including product discontinuation...Knowledge management is a systematic approach to acquiring, analysing, storing, and disseminating information related to products, manufacturing processes and components.”

Efforts to ensure fitness for intended use should focus on those aspects that are critical to patient safety, product quality, and data integrity. These critical aspects should be identified, specified, and verified.

Systems within the scope of this Guide support a wide range of processes, including but not limited to clinical trials, toxicological studies, API production, formulated product production, warehousing, distribution, and pharmacovigilance.

For some manufacturing systems, process requirements depend on a thorough understanding of product characteristics. For these systems, identification of Critical Quality Attributes (CQAs) and related Critical Process Parameters (CPPs) enable process control requirements to be defined.

Specification of requirements should be focused on critical aspects. The extent and detail of requirement specification should be commensurate with associated risk, complexity, and novelty of the system. Requirements may be developed iteratively or incrementally, based upon an initial set of base requirements.

Incomplete process understanding hinders effective and efficient compliance and achievement of business benefit.

2.1.2 Life Cycle Approach within a QMS

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 company's QMS, which should be maintained and kept up-to-date as new ways of working are developed.

As experience is gained in system use, the QMS should enable continual process and system improvements based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Identified improvements and corrective actions should follow change management.

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

The life cycle approach is fundamental to this Guide and embodies each of the other key concepts. The life cycle is structured into phases and activities, as described in Chapter 3.

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 nature of system components including maturity and level of configuration or customization)
- Outcome of supplier assessment (supplier capability)

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

The strategy should be clearly defined in a plan and follow established and approved policies and procedures.

2.1.4 Science-Based Quality Risk Management

QRM is a systematic process for the identification, assessment, control, communication, mitigation, and review of risks.

Application of QRM enables effort to be focused on critical aspects of a computerized system in a controlled and justified manner.

QRM should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity. Combining knowledge management and QRM will facilitate achievement of QMS objectives by providing the means for science- and risk-based decisions related to product quality. For systems controlling or monitoring CPPs, these should be traceable to CQAs, and ultimately back to the Quality Target Product Profile (QTPP) and relevant regulatory submissions.

Qualitative or 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.

A practical risk-management process is described in Chapter 5.

2.1.5 Leveraging Supplier Involvement

Regulated companies should seek to maximize supplier involvement throughout the system life cycle in order to leverage knowledge, experience, and documentation, subject to satisfactory supplier assessment.

For example, the supplier may assist with requirements gathering, risk assessments, the creation of functional and other specifications, system configuration, testing, support, and maintenance.

Planning should determine how best to use supplier documentation, including existing test documentation, to avoid wasted effort and duplication. Justification for the use of supplier documentation should be provided by the satisfactory outcome of supplier assessments, which may include supplier audits.

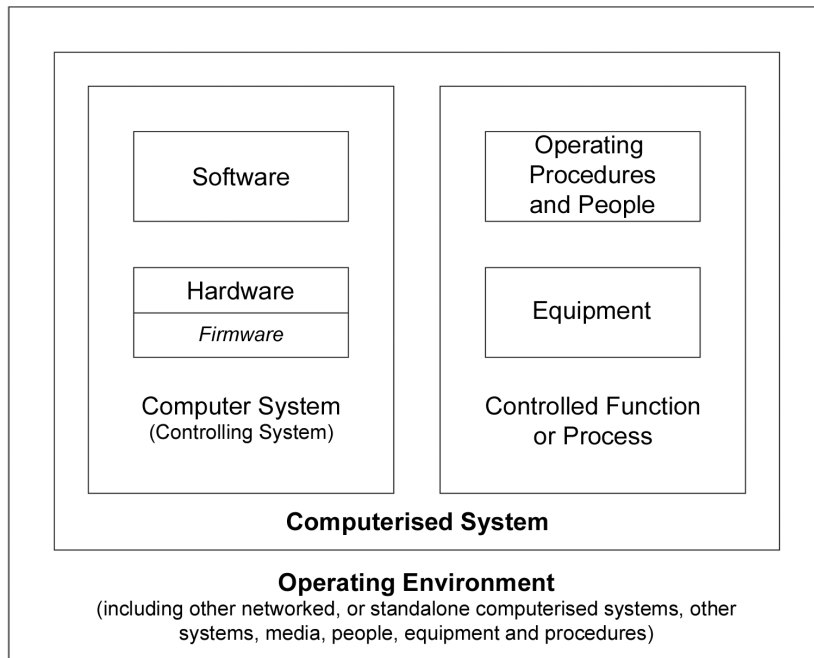
Documentation should be assessed for suitability, accuracy, and completeness. There should be flexibility regarding acceptable format, structure, and documentation practices.

Supplier assessment is described in Chapter 6.

2.2 Key Terms

Computerized System

A computerized system consists of the hardware and software components, together with the controlled function or process (including procedures, people, and equipment and associated documentation) (see also Appendix M11).

Figure 2.2: Computerised System – PIC/S Guidance [22]

This term covers a broad range of systems, including, but not limited to:

- Clinical trials data management
- Manufacturing resource planning
- Laboratory information management
- Automated manufacturing equipment
- Automated laboratory equipment
- Process control and process analysis
- Manufacturing execution
- Building management
- Warehousing and distribution
- Blood processing management
- Adverse event reporting (vigilance)
- Document management
- SaMD and digital health applications

Computerized System Validation

Achieving and maintaining compliance with applicable GxP regulations and fitness for intended use by:

- The adoption of principles, approaches, and life cycle activities within the framework of validation plans and reports
- The application of appropriate operational controls throughout the life of the system

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 [23], US PHS Act [24], FDA regulations [25], EU Directives [26], UK MHRA regulations [27], Japanese regulations [28], or other applicable national legislation or regulations under which a company operates.

These include but are not limited to (further descriptions provided in Appendix G2):

- GMP
- GCP
- GLP
- GDP
- Good Quality Practice (GQP)
- Good Pharmacovigilance Practice (GVP)
- Medical Device Regulations
- Prescription Drug Marketing Act (PDMA) [29]

Process Owner

This is the owner of the business process or processes being managed. The process owner is ultimately responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable company Standard Operating Procedures (SOPs). The process owner may also be the system owner. The process owner may be the *de facto* owner of the data residing on the system (data owner) and therefore, ultimately responsible for the integrity of the data. Process owners are typically the head of the functional unit using the system. (cf. System Owner)

Quality Management System (QMS)

Management system to direct and control an organization with regard to quality. (ISO [7]).

(This is equivalent to **Quality System** as defined in ICH Q9 [14].)

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 [8])

System Owner

The system owner is responsible for the availability and support and maintenance of a system, and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable company SOPs. The system owner also may be the process owner (e.g., for IT infrastructure systems or systems not directly supporting GxP). For systems supporting regulated processes and maintaining regulated data and records, the ownership of the data resides with the GxP process owner, not the system owner.

The system owner acts on behalf of the users. The system owner for larger systems will typically be from IT or engineering functions. Global IT systems may have a global system owner and a local system owner to manage local implementation. (cf. Process Owner)

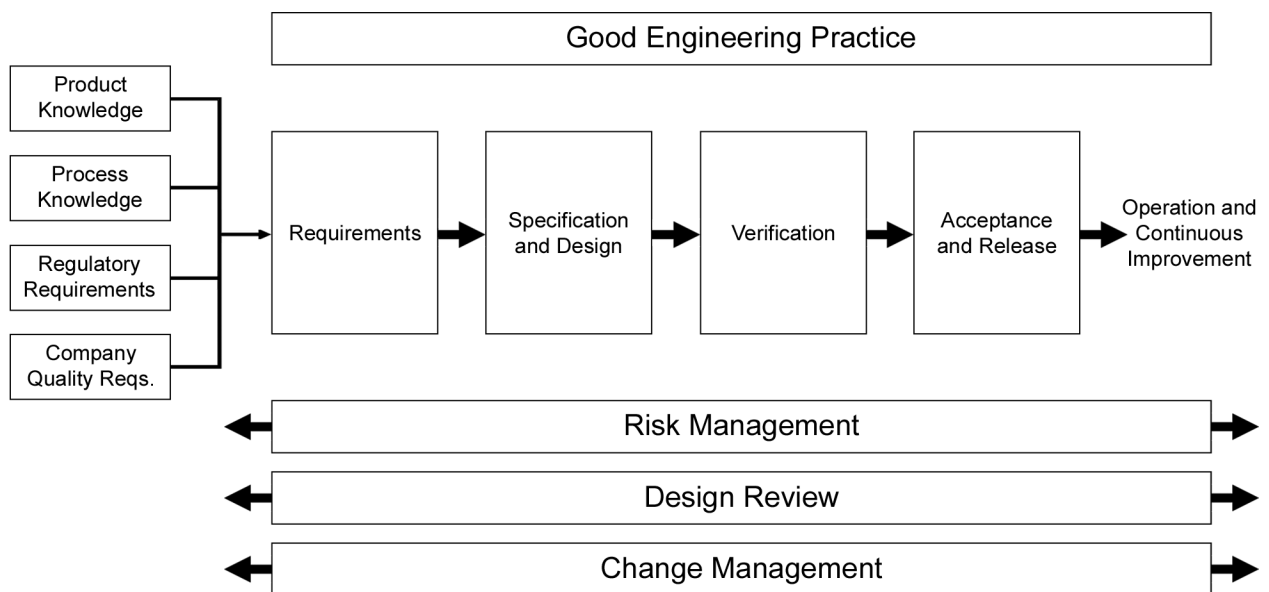
3 Life Cycle Approach

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, understanding the requirements, through development, release, and operational use, to system retirement. Figure 3.1 shows a general specification, design, and verification process described in ASTM E2500 [8].

Figure 3.1: The Specification, Design, and Verification Process [8]

Reprinted with permission from ASTM E2500-20 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment, copyright ASTM International, 100 Barr Harbor Dr., West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM at www.astm.org.



This section of the Guide introduces the computerized system life cycle, a general approach to specification and verification, a framework for computerized system validation, and the application of critical thinking.

3.1 Computerized System Life Cycle

The computerized system life cycle encompasses all activities from initial concept to retirement.

The life cycle for any system consists of four major phases:

- Concept
- Project
- Operation
- Retirement

During the concept phase, the regulated company should consider opportunities to automate one or more business processes based upon business need and benefits. Typically at this phase, initial requirements will be developed and potential solutions considered. From an initial understanding of scope, costs, and benefits, a decision is made on whether to proceed to the project phase. An initial risk assessment or GxP assessment should be performed, so that GxP regulated systems are identified before the project phase commences.

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.

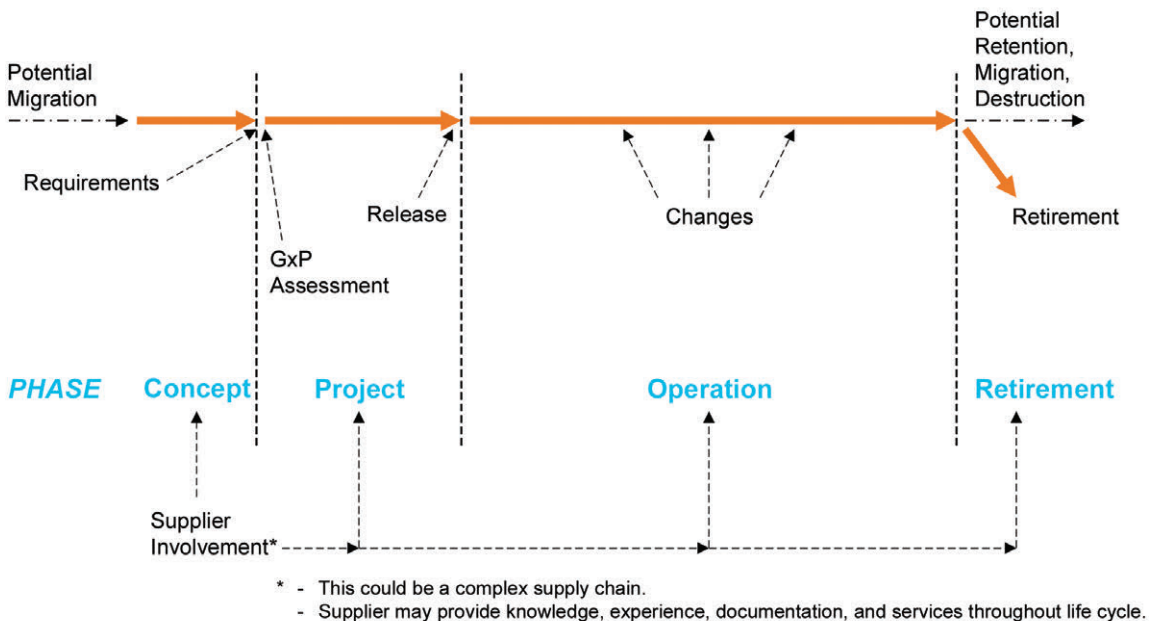
System operation is often the longest phase and is managed using defined, up-to-date, operational processes and procedures applied by personnel who have appropriate training, education, and experience. Maintaining control (including security), fitness for intended use, and compliance are key aspects. The management of changes of different impact, scope, and complexity is an important activity during this phase.

The final phase is the ultimate retirement of the system. It involves decisions about data retention, migration, or destruction, and the management of these processes.

Suppliers of products and services should be involved as appropriate throughout the life cycle. It may be appropriate to delegate many of the described activities to suppliers, subject to satisfactory supplier assessment and control measures.

These life cycle phases are shown in Figure 3.2.

Figure 3.2: Life Cycle Phases



An inventory of computerized systems should be maintained. Further details are given in Chapter 6. A GxP assessment should be performed by the beginning of the project stage to determine whether a system is GxP regulated, and if so, which specific regulations apply, and to which parts of the system they are applicable. This should be performed as part of the initial system risk assessment (Step 1 as described in Chapter 5). For similar systems, it may be appropriate to base the GxP assessment on the results of a previous assessment provided the regulated company has an appropriate established procedure.

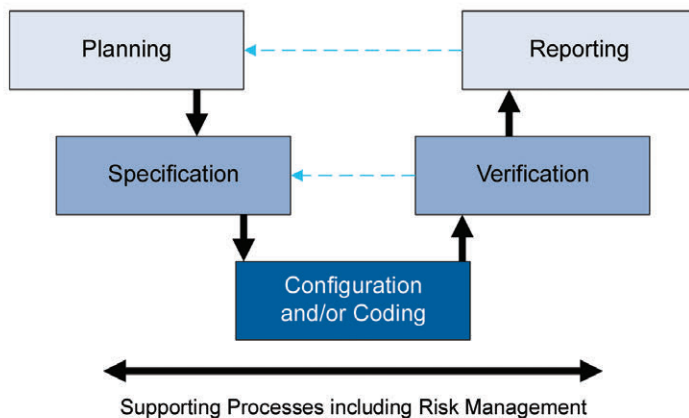
The computerized system life cycle described in this section should not be confused with the need for a defined approach or method for software development by the supplier. Chapter 7 discusses supplier activities in more detail.

3.2 Specification and Verification

The GAMP specification and verification approach is not inherently linear; it also fully supports iterative and incremental (Agile) methods, as shown below.

A linear approach is particularly suitable when system requirements are fully understood and defined upfront. Figure 3.3 shows a linear approach for achieving computerized system compliance and fitness for intended use within the system life cycle. The specification activities have equivalent verification steps to determine whether the specification has been met. A hierarchy of specifications may be required for larger systems, while specifications may be combined for smaller, simpler, or standard systems. Specifications are addressed by appropriate verification steps.

Figure 3.3: Linear Approach to Achieving Compliance and Fitness for Intended Use



The application of this general approach will vary widely depending on the risk, complexity, and novelty of the system. Specific examples showing typical activities for different types of systems are provided in Chapter 4.

As shown in Figure 3.4, the life cycle and specification and verification approach described in the Guide is not inherently linear.

Figure 3.4: Iterative and Incremental Approach to Achieving Compliance and Fitness for Intended Use [20]



This Guide supports the use of Agile approaches for product development, the development of custom applications, and incremental product configuration. Factors for the successful adoption of Agile include a robust QMS within an appropriate organizational culture, well-trained and highly disciplined teams following a well-defined process supported by effective tools and automation, and proper customer or product owner involvement. (See also Appendix D8)

This Guide describes the overall GxP system life cycle from the perspective of the regulated company and does not define the software development process in detail.

While this section provides a suggested approach for activities performed by a regulated company, it is recognized that other models and approaches are equally acceptable.

3.3 Computerized System Validation Framework

GAMP advocates a computerized system validation framework to achieve and maintain GxP compliance throughout the computerized system life cycle.

The framework is based on system-specific validation plans and reports and the application of appropriate operational controls. Validation plans and reports provide a disciplined and consistent approach to meeting regulatory requirements, leading to appropriate documentation at the right level. Such documents are valuable both in preparing for, and during, regulatory inspections.

The framework is applicable for the majority of computerized systems. This Guide has built on these principles by clarifying the scalability of the approach, and the central role of QRM, to effectively and efficiently cover the very wide range of systems in scope.

Where a computer system is regarded as one component of a wider manufacturing process or system, particularly in an integrated QbD environment, specific and separate computerized system validation may not be necessary. This environment requires both complete product and process understanding and that the CPPs can be accurately and reliably predicted and controlled over the design space. In such a case, the fitness for intended use of the computer system within the process may be adequately demonstrated by documented engineering or project activities together with subsequent process validation or continuous quality verification of the overall process or system. The same principle applies to the adoption of Process Analytical Technology (PAT).

For automated manufacturing equipment, separate computer system validation should be avoided. Computer system specification and verification should be part of an integrated engineering approach to ensure compliance and fitness for intended use of the complete automated equipment. Further information can be found in *ISPE Baseline® Guide: Volume 5 – Commissioning and Qualification (Second Edition)* [30].

This framework is described in Appendix M1 and Appendix M7.

3.4 Critical Thinking Through the Life Cycle

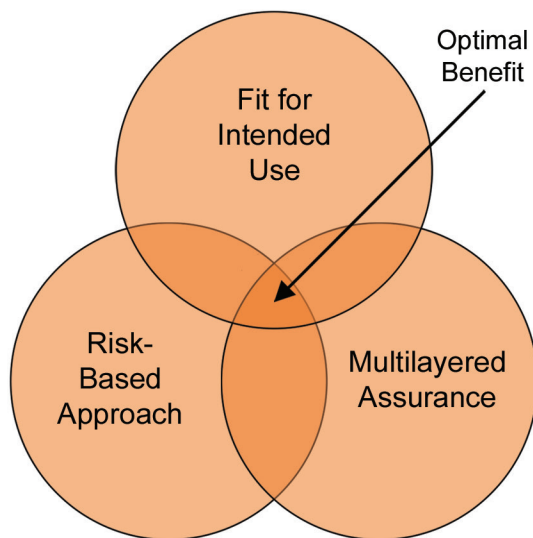
Critical thinking promotes informed decision-making and good judgment on where and how to apply and scale quality and compliance activities for computerized systems. It relies on knowledge of the business process and on the detailed comprehension and analysis of where the business process can potentially impact patient safety, product quality, and data integrity. A better understanding of risks results in more confidence in the assessment and control of those risks, and therefore supporting robust scaling of controls and validation activities.

The extent and depth, formality, and level of documentation formality may, and should, vary to a considerable degree between different business processes, types of systems, functions within a system, and applications. Significant efficiency improvements can be achieved by focusing on what is essential in individual situations and avoiding unnecessary work. Critical thinking is not a one-time activity and should be applied throughout the computerized system life cycle. As such, critical thinking should become a habitual mindset based on an intellectual commitment to continual improvement.

Figure 3.5 illustrates critical thinking for computerized systems whereby proactive adoption of a risk-based approach suitable for the intended use of the computerized system takes into account the multiple layers of assurance provided elsewhere within the business process. In other words, combining technical, procedural, and behavioral controls applied throughout the business process is used when assessing the risk of the computerized system. These layers of assurance may exist upstream or downstream of the system within the business process it supports and include supplier activities [20].

This holistic approach requires an initial investment of time and effort to analyze the overall business process that the computerized system will support, and the associated regulated data. For example, the value of strong, validated data integrity technical controls in the system could be negated by errors caused by manual transcription of regulated data into the system. Data integrity cannot be recovered once lost. Business process mapping and data flow diagrams capture this knowledge and facilitate the identification and understanding of the potential risks to patient safety, product quality, and data integrity to determine where assurance is most needed.

Figure 3.5: Critical Thinking for Computerized Systems [20]



Regulatory authorities are adopting critical thinking to help determine whether controls are fit for intended use to ensure patient safety, product quality, and data integrity. Practitioners should not consider that the level of regulatory compliance achieved is directly proportionate to the amount of paperwork produced. Too much paperwork can confuse and make it harder to maintain and inspect computerized systems. Regulators look for scaled and targeted activities with well-organized information and records that have an appropriate level of detail, supported by clear and unambiguous rationales explaining the critical thinking applied. The information/records contained within software development and support tools offer the opportunity to demonstrate control in areas where separate documentation was previously considered a necessity, and these should be leveraged [31]. (See also Appendix D9)

Further information can be found in Appendix M12 and the *ISPE GAMP® Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management* [20].

4 Life Cycle Phases

This section further describes the phases of the computerized system life cycle introduced in Chapter 3.

The life cycle approach described is not inherently linear, and is designed to be compatible with a wide range of models and methods, including iterative and incremental (Agile) approaches. References to documentation and deliverables should not be interpreted as always requiring traditional documents. The maintenance of records and information in appropriate and effective software tools is encouraged.

4.1 Concept

Detailed activities in this phase will depend on company approaches to initiating and justifying project commencement. Gaining management commitment to provide appropriate resources is an important pre-project activity. An initial risk assessment or GxP assessment should be performed so that GxP regulated systems are identified before the project phase commences.

4.2 Project

This section describes the following project stages in more detail:

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

The key supporting processes of risk management, change and configuration management, design review, traceability, and document management also are described in this section.

Figure 4.1 shows how these project stages and supporting processes form part of the computerized system life cycle. The stages are equally applicable to the project phase and to subsequent changes during operation.

This is a simplified general model that describes a staged approach to the project phase. For example, it covers both configuration and coding, which are required only for certain types of systems. Specific examples of how to use this staged approach for typical types of systems are specified in Section 4.2.6.

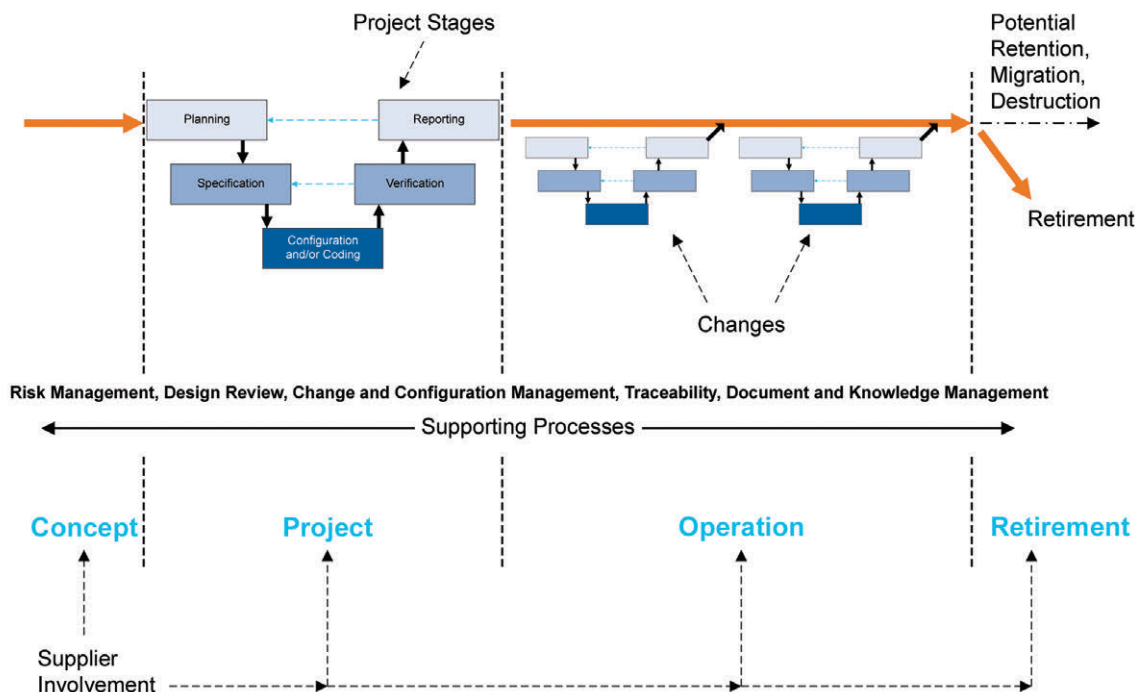
Each project stage typically involves multiple activities; for example, planning may involve:

- Preparing project plans
- Establishing project teams
- Developing requirements
- Conducting supplier assessments
- Defining the extent and formality of verification activities

While the project phase is made up of generally sequential stages, detailed activities often will be performed in parallel or with some overlap. For example, verification activities may occur through several stages. Iterative and incremental approaches may also be used.

Information produced during the execution of these stages provide the evidence that the system is fit for its intended use. Some of this may be used by the regulated company during regulatory inspections to provide justification of the suitability of the system.

Figure 4.1: Project Stages and Supporting Processes within the Life Cycle



4.2.1 Planning

Planning should cover all required activities, responsibilities, procedures, and timelines.

As described in Section 2.1.3, 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 nature of system components, including maturity and level of configuration or customization)
- Outcome of supplier assessment (supplier capability)

For further details on computerized system validation planning, see Appendix M1. In some cases, specific computerized system validation plans may not be required as described in Section 3.3.

A clear and complete understanding of the process to be supported and initial user requirements facilitates effective planning. Initial requirements are often gathered during the concept phase and refined and enhanced during the planning stage.

The extent and detail of requirements gathering and specification should be sufficient to support risk assessment, further specification, development of the system, and verification. These activities may be linear or iterative and incremental (Agile). Comparison of available solutions may result in refinement of the requirements.

The approach should be based on product and process understanding and relevant regulatory requirements. Where appropriate, e.g., for process control systems, requirements should be traceable to relevant CPPs and CQAs.

Requirements are the responsibility of the user community and should be maintained and controlled.

See Appendix D1 for further details on Requirements Specifications (RS).

4.2.2 Specification, Configuration, and Coding

The role of specification 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 company for non-custom products.

Specifications should be adequate to support subsequent activities, including risk assessment, further specification and development of the system, verification as appropriate, and system maintenance and update.

The requirements for configuration and coding activities depend on the type of system (see Section 4.2.6 for examples).

Any required configuration should be performed in accordance with a controlled and repeatable process. Any required software coding should be performed in accordance with defined standards. The need for code reviews within the organization producing the software should be considered.

Configuration management and version control are intrinsic and vital aspects of controlled configuration and coding.

Figure 4.1 shows specification as a separate activity to configuration and coding. However, specification activities may be distinct from, or tightly linked to, configuration and coding activities depending on the software development method being adopted.

Specifications should be maintained and controlled. See Appendix D1 and Appendix D3 for further details on specification, configuration, and design. See Appendix D4 for further details on the management, development, and review of software.

4.2.3 Verification

Verification confirms that specifications have been met. This may involve multiple stages of reviews and testing depending on the type of system, the development method applied, and its use.

While verification is shown as a single box on Figure 4.1, verification activities occur throughout the project stages. For example, design reviews should verify specifications during the specification stage. See Section 4.2.5 for further details on design reviews.

Terminology used to cover verification activities is described in Section 4.2.6.4.

Testing computerized systems is a fundamental verification activity. Testing is concerned with identifying defects so that they can be corrected, as well as demonstrating that the system meets requirements.

The use of effective and appropriate testing tools is encouraged. Such tools should have documented assessments for their adequacy (refer to EU Annex 11 Clause 4.7 [32]) and be controlled in use; however, validation is not required.

Testing is often performed at several levels depending on the risk, complexity, and novelty. Different types of testing are covered in Appendix D5, Section 6.

Tests may be defined in one or more test specifications to cover hardware, software, configuration, and acceptance.

An appropriate test strategy should be developed based on the risk, complexity, and novelty. Supplier documentation should be assessed and used if suitable. The strategy should define which types of testing are required and the level and purpose of test specifications. The test strategy should be reviewed and approved by appropriate SMEs.

See Appendix D5 for further details on testing and development of an appropriate test strategy.

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 in GxP regulated activities should follow a defined process and involve oversight and input of the process owner, system owner, and the appropriate quality function as necessary and applicable. This may be a continuously managed process rather than a one-off event, for example Continuous Integration and Continuous Deployment (CI/CD), and Software as a Service (SaaS).

A computerized system validation report should be produced summarizing the activities performed, any deviations from the plan, any outstanding and corrective actions, and provide a statement of fitness for intended use of the system. See Appendix M7 for further details.

The incorporation of lessons learned/after action review stage gates in the project should be considered (see *ISPE Good Practice Guide: Knowledge Management in the Pharmaceutical Industry*, Appendix 6 [10]).

In some cases, specific computerized system validation reports may not be required, as described in Section 3.3.

A well-managed system handover from the project team to the process owner, system owner, and operational users is a prerequisite for effectively maintaining compliance of the system during operation. See Section 8.6 and Appendix O1 for further details on system handover.

4.2.5 Supporting Processes

4.2.5.1 Risk Management

An appropriate risk-management process should be established.

See Chapter 5 and Appendix M3 for further details on risk management.

4.2.5.2 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 during its life cycle.

Change management procedures covering software, hardware, and documentation 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.

Any involvement of the supplier in these processes should be defined and agreed.

See Appendix M8 for further details on project change and configuration management.

4.2.5.3 Design Review

At suitable stages during the life cycle, planned and systematic design reviews of specifications, design, and development should be performed. This design review process should evaluate deliverables to ensure that they satisfy the specified requirements. Corrective actions should be defined and progressed.

The rigor of the design review process and the extent of documentation should be based on risk, complexity, and novelty.

Design reviews are mainly applicable for custom applications and within the supplier product development processes.

See Appendix M5 for further details on design reviews.

4.2.5.4 Traceability

Traceability is a process for ensuring that:

- Requirements are traceable back to business process needs
- 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 greatly assist the assessment and management of change.

Traceability should be focused on aspects critical to patient safety, product quality, and data integrity. The use of traceability tools and automated traceability methods is encouraged.

See Appendix M5 for further guidance on traceability.

4.2.5.5 Documentation Management and Knowledge Management

Management of documentation includes preparation, review, approval, issue, change, withdrawal, and storage. See Appendix M9 for further details on documentation management. Information and records may be maintained in appropriate and effective tools rather than in traditional documents.

Documentation, tools, and systems contain explicit knowledge that is captured and codified, whereas implied knowledge is context-specific knowledge acquired through personal experience or internalization rather than physical media or information systems. Both need to be considered for successful initial and subsequent system deployments.

See the *ISPE Good Practice Guide: Knowledge Management in the Pharmaceutical Industry* [10] for further details on knowledge management.

4.2.6 Practical Examples

This section shows how the general approach may be applied in a scalable manner to three common types of systems, using Categorization of software. Categorization assists in selecting appropriate life cycle activities and deliverables, as described in Appendix M4, based on the nature of the component and likelihood of defects.

Computerized systems are generally made up of a combination of components from different GAMP Categories (as described in the following subsections). For example, core functionality within a computerized system may be Category 3, with Category 4 workflow configuration, and custom interfaces to other systems being Category 5.

Categories 3 to 5 should be viewed as a continuum with no absolute boundaries. The software category is just one factor to consider in a risk-based approach. Life cycle activities should be scaled based on the GxP impact, complexity, and novelty of the system. In all cases, the emphasis should be on ensuring fitness for intended use based on appropriate technical activities following current good practice. Table-driven approaches purely based on categorization decisions should be avoided.

For convenience the activities shown in this section are a linear representation, but iterative and incremental (Agile) approaches are equally acceptable as described in Section 3.2 and Appendix D8.

These examples are intended to be indicative and for illustration purposes only. Actual approaches for specific systems should be based on the results of supplier assessments and risk assessments, in addition to the categorization of system components, as described in Appendices M2, M3, and M4.

The terminology used in these examples is discussed in Section 4.2.6.4.

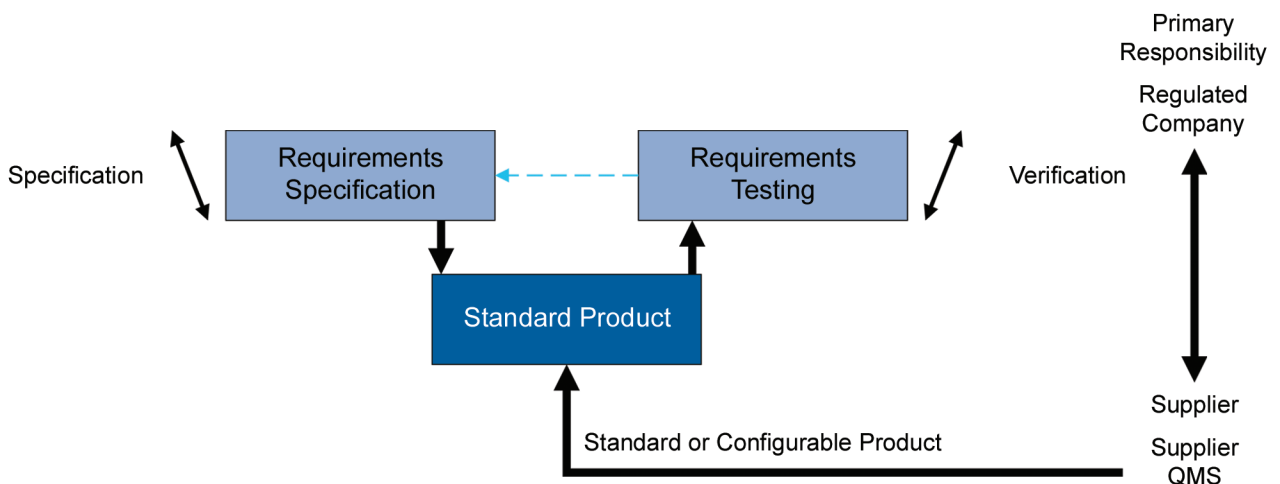
4.2.6.1 Example of a Standard Product

Many computerized systems comprise commercially available software products running on standard hardware components.

Software products that are used off-the-shelf (i.e., standard and not configurable for a specific business process), are typically classified as GAMP Category 3. This includes off-the-shelf components used for business purposes. It includes both those that cannot be configured to conform to business processes, and those that offer defined ranges of factory-provided values or ranges (also called parameterization, as may be found in process control systems and simple laboratory devices). In both cases, configuration to run in the user's environment is possible and likely (e.g., for printer setup).

In such cases, and based on satisfactory supplier and risk assessments, a simple approach consisting of one level of specification and verification is typically applicable (see Figure 4.2).

Figure 4.2: Approach for a Standard Product (Category 3)



Testing typically covers:

- Correct installation
- Tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- Any further tests as a result of risk and supplier assessments

Regulated companies typically perform the required specification and verification. While the system is not configured for a business process, there may be some limited configuration such as run-time parameters or printer setup.

Supplier activities typically include supply of the product, and provision of documentation, training, and support and maintenance.

4.2.6.2 Example of a Configured Product

A common type of computerized system involves the configuration of commercially available software products running on standard hardware components. These may be installed on-premise by the regulated company, or increasingly for IT applications such as SaaS, hosted by an IT service provider/supplier.

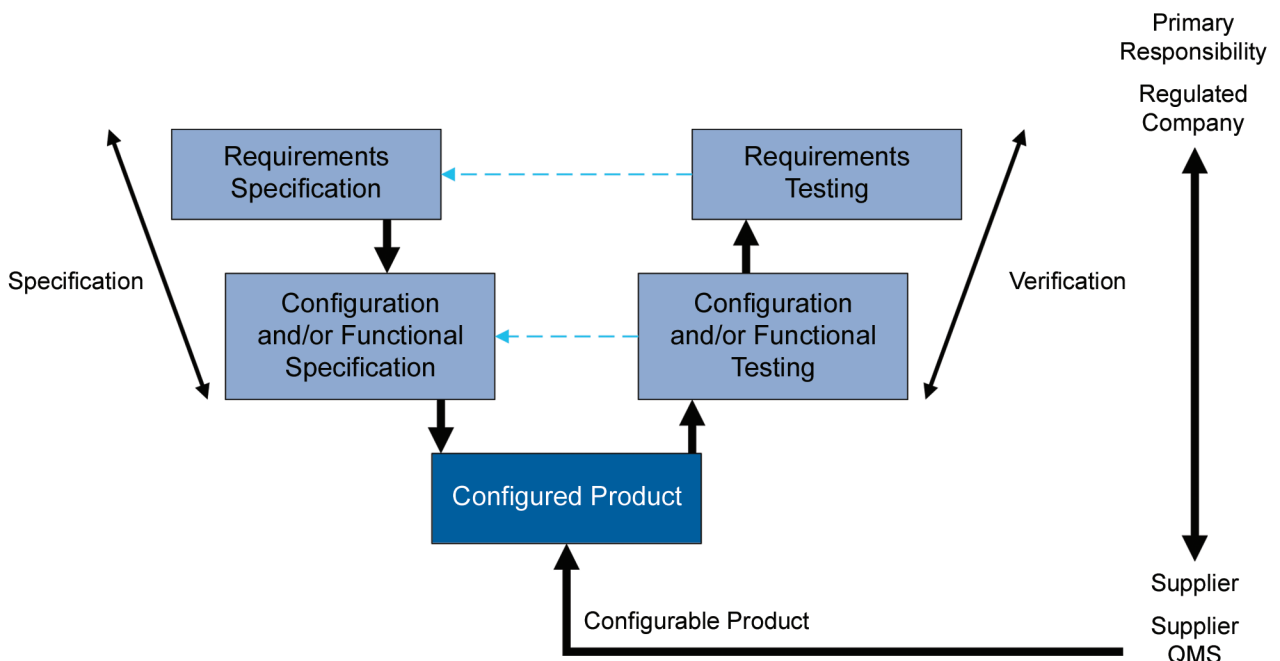
Commercial software products that are configured for a specific business process are typically classified as GAMP Category 4.

In such cases, and based on satisfactory supplier and risk assessments, a flexible approach to specification and verification may be applied. The number of deliverables required to cover the required specification and verification of functionality delivered via configuration will depend on the size, complexity, and technical architecture of the system (see Figure 4.3). For example, in many cases, functionality and configuration aspects may be combined into one specification, or the definition of configuration to meet defined requirements is all that is required.

In some cases, for example, complex on-premise solutions such as process control systems, but not typically for commercially available IT products or SaaS solutions, a project-specific functional specification and subsequent functional testing may be defined and agreed between the regulated company and the supplier.

The illustrative diagrams in this section show the project phase activities from the regulated company perspective. Reference to functional and other project specifications should not be confused with the supplier's internal core product functional specifications, technical, architectural, and design specifications that are maintained within the supplier QMS as part of their product life cycle information.

Figure 4.3: Approach for a Configured Product (Category 4)



Testing typically covers:

- Correct installation
- Configuration of the system

- Functionality that supports the specific business process based on risk and supplier assessments (this is an area where supplier activities may and should be leveraged as much as possible, see Section 8.3)
- Tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- Any further tests as a result of risk and supplier assessments

Regulated companies should decide upon the required levels of specification and verification, and many of the project phase activities and documents may be delegated. Since the system is configured for a business process, testing should be focused on this configuration.

Supplier activities typically include:

- Supply of the product
- Production of specifications and test specifications, as required, on behalf of the regulated company
- Support during configuration and testing
- User documentation
- Training
- Support and maintenance activities

The supply of the product and configuration may be performed by different suppliers.

Note that projects that are predominantly Category 4 may also require development of new custom software components, such as interfaces.

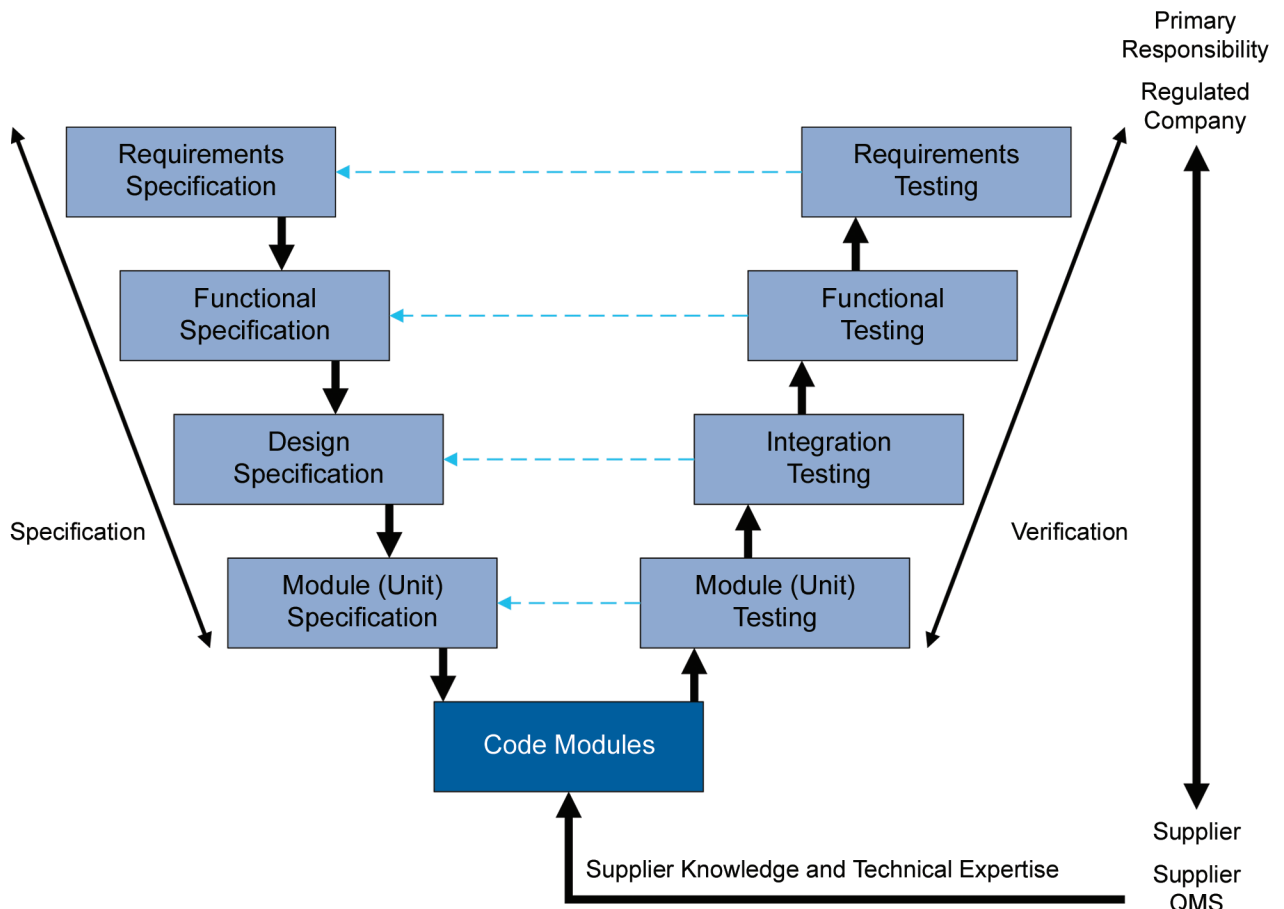
4.2.6.3 Example of a Custom Application

Some computerized systems are developed to meet individual user requirements, where no commercially available solution is suitable. These may be developed using a linear (waterfall) approach or by using iterative and incremental (Agile) methods. (See Figure 4.4)

The software developed for such systems is classified as GAMP Category 5.

In complex cases an approach consisting of various levels of specification and verification may be applied. The number of deliverables required to cover these levels will depend on the complexity and impact of the system. For example, for a small simple system the specification and design specifications may be combined. References to documentation and deliverables should not be interpreted as always requiring traditional documents, and the maintenance of records and information in appropriate and effective software tools is encouraged. For automated process equipment, computer system specification and verification should be part of an integrated engineering approach to ensure compliance and fitness for intended use.

Figure 4.4: Approach for a Custom Application (Category 5)



Testing typically covers:

- Correct installation
- Functionality and design
- Tests that demonstrate fitness for intended use and allow acceptance of the system against requirements
- Any further tests as a result of risk assessments and supplier assessments

Regulated companies should decide upon the required levels of specification and verification, and many of the project phase activities and deliverables may be delegated. Since the system is new, rigorous testing should be performed at both functional and design levels.

Supplier activities typically include production of specifications and test specifications on behalf of the regulated company, development of new software, testing, user documentation, training, and support and maintenance activities.

Complex systems may require a further hierarchy of specifications covering hardware design specifications and configuration specifications.

4.2.6.4 Terminology

The specific terminology used to describe life cycle activities and deliverables varies from company to company and from system type to system type. There are a number of reasons for this, including:

- Regulated companies having different approaches
- Difference in emphasis of GLP, GCP, GMP, GVP, and medical devices
- Difference in emphasis of various regulatory agencies
- Different international or local standards being followed
- Different types of computerized systems (e.g., IT, manufacturing, and laboratory systems)
- Suppliers using a range of different development models and approaches

This Guide aims to be flexible and does not intend to prescribe any one set of terms to the exclusion of others.

This section describes how qualification terminology, as traditionally used, relates to the activities described in this Guide. See Table 4.1. This will assist readers who use this terminology with the application of this Guide.

This Guide does not use traditional pharmaceutical process validation terminology such as IQ/OQ/PQ to describe system life cycle activities. This aligns with the US FDA, who also chose not to use the terminology in General Principles of Software Validation; Final Guidance for Industry and FDA Staff [33] because the terminology may not be well understood among many software professionals. This qualification terminology is also not well aligned with current good software engineering and IT/IS practice, or typical software supplier practices, and implies an inherently linear approach. Such terminology may, however, be appropriate for the qualification of, for example, simpler stand-alone manufacturing or laboratory equipment.

Whatever terminology is used for verification activity, the overriding requirement is that the regulated company 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 (DQ)	Documented verification that the proposed design of facilities, systems, and equipment is suitable for the intended purpose	Design review (See Section 4.2.5 for further details)
Installation Qualification (IQ)	Documented verification that a system is installed according to written and approved specifications	Checking, testing, or other verification to demonstrate correct: <ul style="list-style-type: none"> • Installation of software and hardware • Configuration of software and hardware (See Appendix D5 for details)
Operational Qualification (OQ)	Documented verification that a system operates according to written and 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. (See Appendix D5 for details)

Table 4.1: Relationship between Traditional Qualification Terminology and GAMP 5 Activities (continued)

Traditional Term	Description	GAMP 5 Verification Activity
Performance Qualification (PQ)	Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and 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. (See Appendix D5 for details)

Note: The use of qualification terminology in relation to computerized systems and the relationship between OQ and PQ in particular, varies from company to company. The comparisons in Table 4.1 provide a general interpretation only and are not intended to be prescriptive.

Regulated companies should decide on a verification approach appropriate to a specific system. Testing activities should be selected based on the risk, complexity, and novelty of the system as described in Section 4.2.3.

The examples in Section 4.2.6 illustrate the typical different levels of testing applied to different categories of system, such as:

- Module testing
- Integration testing
- Configuration testing
- Functional testing
- Requirements testing

Table 4.1 lists various GAMP verification activities. There is no one-to-one relationship between the levels of testing and the GAMP verification activities, as the following examples show. Note that these examples are intended as illustrative and not prescriptive, and that critical thinking and technical experience and knowledge should be applied to the selection of the appropriate life cycle approach.

- For a typical Category 3 system, testing of both installation and configuration are covered by requirements testing.
- For a typical Category 3 system, tests are executed to demonstrate fitness for intended use and to allow acceptance of the system against user requirements. There is typically no need for further testing to demonstrate correct operation of standard functionality of the product.
- For a typical Category 4 system, while testing of configuration is covered by configuration testing, testing of installation may occur at any of the testing levels depending on the project.
- For a typical Category 5 system, correct operation of functionality that supports the specific business process may be covered by module testing, integration testing, and functional testing, and may be supplemented by pre-delivery testing.

The relationship between the required verification and the different levels of testing, particularly for GAMP Category 4 and GAMP Category 5 systems, may be complex. The verification or test strategy for a particular system should ensure that the required verification activities are adequately covered.

Acceptance of the system by the regulated company as being fit for release for operational use includes satisfactory completion of an agreed set of verification activities. For some systems, this may occur in stages including the leveraging, wherever possible, of testing or other acceptance activities performed prior to, and after, delivery. Commonly used terms within such a process include Factory Acceptance Testing, Site Acceptance Testing, and System Acceptance Testing. Verification activities should not be duplicated unnecessarily.

Whichever terms are used, the verification strategy should clearly define which activities should be satisfactorily completed to allow acceptance of the system for release into operational use by the regulated company.

See Appendix D5 for further guidance on aspects of testing.

4.3 Operation

This section provides guidance on system operation. Not all the activities will be directly relevant to all systems. The approach and required activities should be selected and scaled according to the nature, risk, and complexity of the system in question through the application of critical thinking.

For more detailed information on system operation topics see the *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [34].

As part of preparing for final acceptance and formal handover for live operation, the regulated company 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.

Depending on the deployment model and degree of outsourcing, the supplier (or service provider) may host and administer, as well as support, the system. Appropriate contracts and agreements are essential to define expectations, responsibilities, and performance measures.

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 established and up-to-date procedures and training that cover use, maintenance, and management.

The operational phase of a system may last many years, and may include changes to services, 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. The use of supporting systems and tools to digitize and automate processes for efficiency, consistency, and process adherence is encouraged.

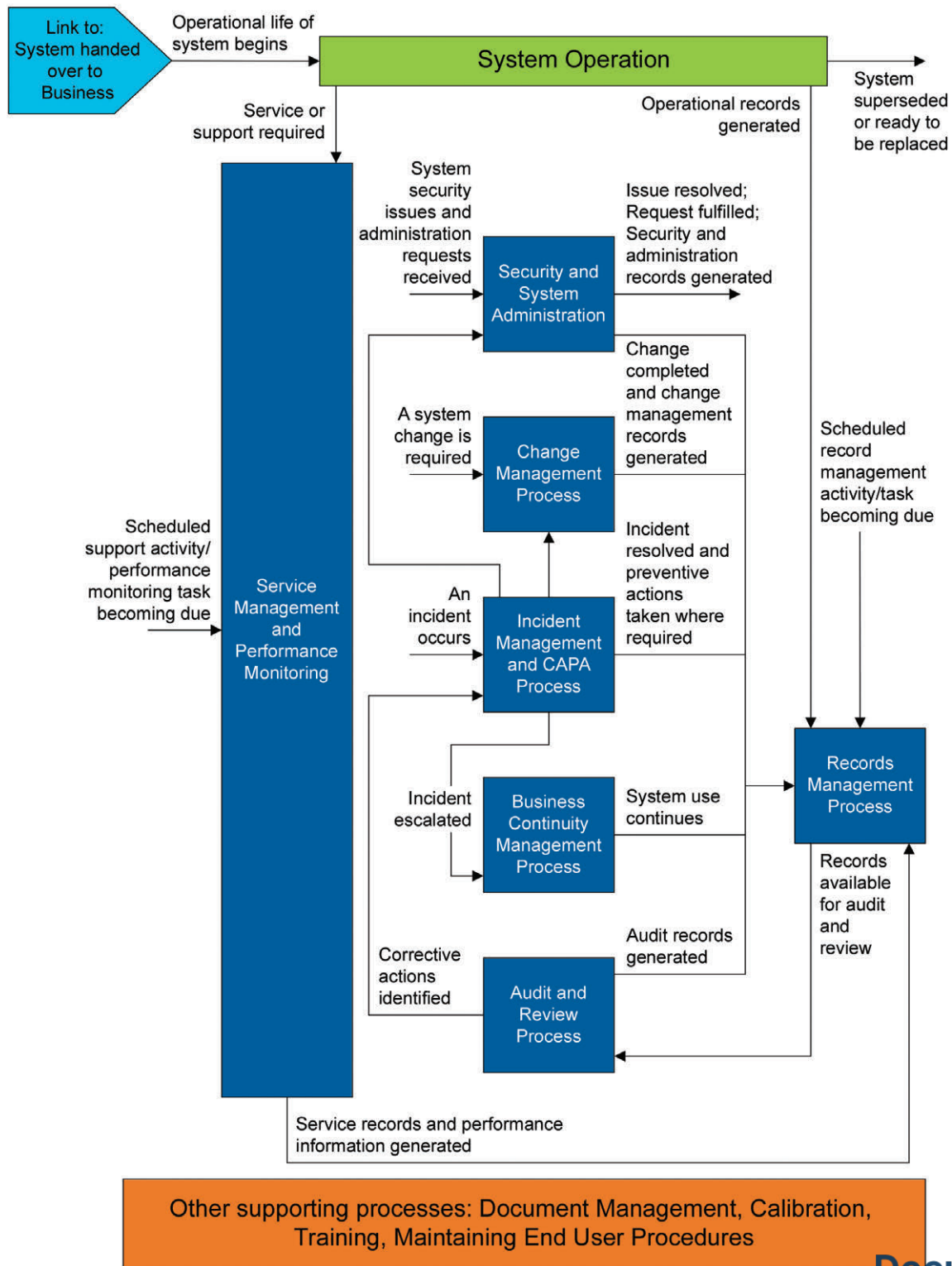
As experience is gained during operation, opportunities for process and system improvements should be sought based on periodic review and evaluation, operational and performance data, and root-cause analyses of failures. Information from the incident and problem management and Corrective and Preventive Action (CAPA) processes can provide significant input to the evaluation.

Change management should provide a dependable mechanism for prompt implementation of technically sound improvements following the approach to specification, design, and verification described in this Guide. The rigor of the approach, including the extent of documentation and verification, should be based on the risk and complexity of the change through the application of critical thinking.

Note that operational GxP computerized systems as discussed in this section are those that support internal regulated company GxP business processes, whereas operational SaMD is typically a product in the hands of patients or health care providers. In these cases further medical device-related requirements such as the need for post-market surveillance also apply.

Maintaining system compliance involves many interrelated activities. Figure 4.5 shows the major relationships between related groups of these activities. Service management and performance monitoring occur throughout the operational life of the system. Other activities, such as change management, occur when triggered.

Figure 4.5: Major Information Flows between Operational Activities



Some of the groups of activities shown in Figure 4.5 contain several individual related processes, procedures, and plans, as described in Table 4.2.

Table 4.2: Grouping of Operational Processes

Group of Processes	Process	Appendix
Handover	Handover	O1
Service Management and System Monitoring	Establishing and Managing Support Services System Monitoring	O2 O3
Incident and Problem Management, Deviation, and CAPA	Incident Management and Problem Management Corrective and Preventive Action	O4 O5
Configuration Management	Operational Change and Configuration Management	O6
Audits and Review	Periodic Review (Internal Quality Audits not covered by GAMP 5)	O8
Continuity Management	Backup and Restore Business Continuity Management	O9 O10
Security and System Administration	Security Management System Administration	O11 O12
Records Management	Archiving and Retrieval	O13

These processes are supported by QMS activities, such as document management, records management, knowledge management, training management, and the maintenance of up-to-date end user procedures. Further information is available in *ISPE GAMP® Guide: Records and Data Integrity* [35] and *ISPE Good Practice Guide: Knowledge Management in the Pharmaceutical Industry* [10]

The individual support and maintenance processes required to maintain the compliance of computerized systems during operation are briefly described below and covered in more detail in the Operational Appendices as shown in Table 4.2.

The use of good IT practices (e.g., ITIL [5]) supported by IT service management tools and automation is encouraged to ensure the efficiency and effectiveness of support processes and an auditable record of support activities.

4.3.1 Handover

Handover is the process for transfer of responsibility of a computerized system from a project team or a service group to the operations team or a new service group.

This is an important process; achieving compliance and fitness for intended use on its own may not be enough to guarantee a successful transfer into the operational phase.

The handover process will typically involve the project team (development group and/or supplier), process owner, system owner, and Quality Unit. The support group should be involved at the earliest opportunity to ensure effective knowledge transfer and establishment of operational procedures. A period of elevated support and maintenance, often referred to as Hypercare Services, may be arranged to facilitate the transfer.

Implied context-specific knowledge acquired through personal experience or internalization, as well as explicit knowledge captured and codified in documentation, tools, and systems should be considered. See *ISPE Good Practice Guide: Knowledge Management in the Pharmaceutical Industry* [10] for further details on knowledge management.

See Appendix O1 for further details.

4.3.2 Service Management and Performance Monitoring

Figure 4.5 shows the major relationships between operational processes. Service management and performance monitoring are shown related to records management due to records generated to demonstrate proper operation and performance of a system. In addition, there is potential interaction with incident and problem management and CAPA and change management when the results of the service or monitoring indicate there are issues that need addressing. For clarity, these interactions are not shown in Figure 4.5.

4.3.2.1 Establishing and Managing Support Services

The support required for each system, and how it will be provided, should be established. Support may be provided by external service providers or internal resources. This process should ensure that service agreements, maintenance plans, SOPs, support systems, and tools are established.

See Appendix O2 for further details.

4.3.2.2 Performance Monitoring

Performance monitoring detects issues that could impact the availability and performance of the system in order to facilitate mitigation before problems occur. Detected issues are managed through the incident management and problem management processes. Monitoring tools and automation are increasingly used to detect potential issues, report issues, and escalate to support organizations for timely intervention and rectification, and are encouraged.

The need for performance monitoring should be considered, and required activities scheduled and documented. This may change during the operational life of a system.

See Appendix O3 and Appendix D9 for further details.

4.3.3 Incident and Problem Management and CAPA

4.3.3.1 Incident Management and Problem 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; whereas problem management involves analyzing root causes and preventing incidents from happening in the future. 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 and problem management processes may be supported by service management tools that support the incident and problem management process, associated action planning, and traceability of actions taken to address the incident or problem.

See Appendix O4 for further details.

4.3.3.2 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 should feed into the overall CAPA system used for GxP operations. When incidents occur, or when opportunities to reduce process/system failures are identified by other means, CAPA should be identified and processes established to ensure that these are implemented effectively. CAPA can provide a solution to problem control as described in ITIL Problem Management [5].

See Appendix O5 for further details.

4.3.4 Change Management

4.3.4.1 Change Management

Change management is a critical activity that is fundamental to maintaining the proper functioning and controlled status of systems and processes. All changes that are proposed during the operational phase of a computerized system, whether related to software (including middleware), hardware, infrastructure, or use of the system, should be subject to a formal change-control process (see Appendix O6 for guidance on replacements). This process should ensure that proposed changes are appropriately reviewed to assess impact and risk of implementing the change. Regression analysis and regression testing may be required. The process should ensure that changes are suitably evaluated, authorized, documented, tested, and approved before implementation, and subsequently closed.

The 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, by application of critical thinking. Some activities such as replacements and routine system administration tasks should be covered by appropriate repair or system administration processes.

Change management should provide a mechanism for prompt implementation of continual process and system improvements based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures.

See Appendix O6 for further details.

4.3.4.2 Configuration Management

Configuration management includes those activities necessary to precisely define a computerized system at any point during its life cycle, from the initial steps of development through to retirement.

A configuration item is a component of the system that does not change as a result of the normal operation of the system. Configuration items should only be modified by application of a change management process. Formal procedures should be established to identify, define, and baseline configuration items, and to control and record modifications and releases of configuration items, including updates and patches.

See Appendix O6 for further details.

4.3.4.3 Repair Activity

The repair or replacement of defective computerized system components, which are often but not exclusively hardware or infrastructure related, should be managed in accordance with a defined process. Such activities should be authorized and implemented within the wider context of the change management process. Many repair activities are emergencies and require rapid resolution, so the incident and change management processes should be designed to allow such activities to occur without delay or increased risk to the operational integrity of the computerized system.

See Appendix O6 for further details.

4.3.5 Periodic Review

Periodic reviews are used throughout the operational life of systems to verify that they remain compliant with regulatory requirements, fit for intended use, and meet company policies and procedures, including those related to data integrity. The reviews should confirm that, for components of a system, the required support and maintenance processes and expected regulatory controls (plans, procedures, and records) are established.

Periodic reviews should be:

- Scheduled at an interval appropriate to the impact and operational history of the system. Risk and other assessments should be used to determine which systems are in scope and the frequency of periodic review.
- Performed in accordance with a predefined process
- Documented with corrective actions tracked to satisfactory completion

See Appendix O8 for further details.

4.3.6 Continuity Management

4.3.6.1 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 the results of that testing documented.

See Appendix O9 for further details.

4.3.6.2 Business Continuity Planning

Business Continuity Planning (BCP) 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, covering local and global infrastructure, data, and the application.

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.

A business continuity plan defines how the business may continue to function and handle data following failure. It also defines the steps required to restore business processes following a disruption and, where appropriate, how data generated during the disruption should be managed. Plans should be prioritized based on patient and business risk, in case of disruption to multiple systems.

The BCP also identifies the triggers for invoking the business continuity plan, roles and responsibilities, and required communication.

See Appendix O10 for further details.

4.3.6.3 Disaster Recovery Planning

As a subset of BCP, plans should be specified, approved, and rehearsed for the recovery of specific systems in the event of a disaster. These plans should detail the precautions taken to minimize the effects of a disaster, allowing the organization to either maintain or quickly resume critical functions. There should be a focus on disaster prevention, e.g., the provision of redundancy for critical systems. Disaster Recovery (DR) plans often require a shared responsibility model between internal organizations of the regulated company (e.g., business, IT) and external service providers (e.g., cloud service providers).

See Appendix O10 for further details.

4.3.7 Security and System Administration

4.3.7.1 Security Management

Computerized systems and data should be adequately protected against willful or accidental loss, damage, or unauthorized change. Procedures for managing secure access, including adding and removing privileges for authorized users, virus management, password management, and physical security measures should be established before the system is approved for use.

Role-based security should be implemented, if possible, to ensure that sensitive data and functions are not compromised. Security management procedures should apply to all users, including administrators, superusers, users, and support staff (including supplier support staff).

Security provisions should ensure that data is protected against unauthorized intrusions including cyber security attacks. Intrusion prevention and detection processes, supported by relevant IT tools and automation, should be in place.

See Appendix O11 for further details.

4.3.7.2 System Administration

Once a system is in operation the users of the system will require support. The system administration process provides administrative support for systems, including performance of standard administration tasks. The extent of this process varies greatly depending on the nature of the system.

See Appendix O12 for further details.

4.3.8 Record Management

4.3.8.1 Retention

Policies for the retention of regulated records should be established, based on a clear understanding of regulatory requirements and existing corporate policies, procedures, standards, and guidelines.

See Appendix O13 for further details.

4.3.8.2 Archiving and Retrieval

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

See Appendix O13 for further details.

The *ISPE GAMP Guide: Records and Data Integrity* [35] and *ISPE GAMP® RDI Good Practice Guide: Data Integrity by Design* [36] give further details on record retention, archive, and retrieval.

4.4 Retirement

This activity covers system withdrawal, system decommissioning, system disposal, and migration of required data.

4.4.1 Withdrawal

Withdrawal is the removal of the system from active operation, i.e., users are deactivated, interfaces disabled. No data should be added to the system from this point forward. Special access should be retained for data reporting, results analysis, and support.

4.4.2 Decommissioning

Decommissioning is a controlled process by which an application or system is removed from use in an organization once it has been retired and/or has become obsolete.

4.4.3 Disposal

Data, documentation, software, or hardware may be permanently destroyed. Each may reach this stage at a different time. Data and documentation may not be disposed of until they have reached the end of the record-retention period, as specified in the company's record-retention policy, following an authorized and documented process.

Due to the volume of data and records involved, retirement can be a major task for IT systems in particular. Consideration should be given to:

- Establishing procedures covering system retirement, including withdrawal, decommissioning, and disposal as appropriate
- Documentary 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
- The need to migrate records to a new system or archive, and the method of verifying and documenting this process
- Ability to retrieve these migrated records on the new system

Further guidance is also provided in the *ISPE GAMP Guide: Records and Data Integrity* [35] and *ISPE GAMP RDI Good Practice Guide: Data Integrity by Design* [36].

See Appendix M10 for further details.

4.4.4 Data Migration

Data migration may be required when an existing system is replaced by a new system, when an operational system experiences a significant change, or when the scope of use of a system is changed. The migration process should be accurate, complete, and verified.

See Appendix D7 for further details.

