

GOOD PRACTICE GUIDE:

Enabling Innovation

*Critical Thinking, Agile,
IT Service Management*



GOOD PRACTICE GUIDE:

Enabling Innovation

*Critical Thinking, Agile,
IT Service Management*

Disclaimer:

The ISPE GAMP® Good Practice Guide: *Enabling Innovation – Critical Thinking, Agile, IT Service Management* seeks to apply ISPE GAMP® 5 principles and current good practice to these areas to promote innovation and advancement. 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.

© 2021 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 978-1-946964-46-5

Preface

The drive within life sciences to improve patient safety and product quality, and provide value to society, while simultaneously reducing costs requires constant and effective innovation. Operating in a highly regulated sector can result in some practitioners applying unthinking, prescriptive, and rigid approaches that are not commensurate to the needs of the process, the nature of the system, and the real risk to the product and the patient.

This *ISPE GAMP® Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management* discusses three topic areas where regulated companies can apply innovation to meet rapidly changing industry needs. This Guide facilitates the effective and efficient use of valuable resources by the application of appropriate and proportionate practices, so that companies can introduce innovative approaches to reduce risk to patient safety, product quality, and data integrity.

This Guide is aligned with the concepts and framework of the *ISPE GAMP® 5 Guide: A Risk-based Approach to Compliant GxP Computerized Systems*.

Acknowledgements

The Guide was produced by a Task Team led by Heather Watson (GlaxoSmithKline, United Kingdom), Chris Clark (TenTenTen Consulting Limited, United Kingdom), and Sion Wyn (Conformity Ltd., United Kingdom). The work was supported by the ISPE GAMP Community of Practice (CoP).

Core Team

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

Mark Cherry	AstraZeneca	United Kingdom
Chris Reid	Integrity Solutions Limited	United Kingdom
Judith Samardellis	Syneos Health	USA
Lorrie Vuolo-Schuessler	Syneos Health	USA
Charlie Wakeham	Waters Corporation	Australia
Guy Wingate	GlaxoSmithKline	United Kingdom

Contributors

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

Karen Ashworth	Karen Ashworth Consulting Ltd.	United Kingdom
Carsten Bierans	Körber Business Area Pharma	Germany
Stephen Ferrell	Compliance Path Ltd.	USA
James Gunning	Johnson Matthey	USA
Frank Henrichmann	QFINITY	Germany
Oliver Herrmann	QFINITY	Germany
Paul James-Martin	Integrity Project Solutions Limited	United Kingdom
Kevin C. Martin	Azzur Group LLC	USA
Andrew McDonagh	Emergn	United Kingdom
Elizabeth McLellan	Suvoda, LLC.	USA
Khaled Moussally	Compliance Group	USA
Ray Murphy	Boston Scientific	USA
Donal O'Brien	Dassault Systèmes	Ireland
Michael Osburn	Cornerstone OnDemand	USA
Randy Perez	Novartis (retired)	USA
Jens Seest	Novartis	Germany
Ken Shitamoto	Gilead Sciences, Inc.	USA
Andy Tyrrell	Cornerstone OnDemand	United Kingdom
Anders Vidstrup	NNIT A/S	Denmark
Mark Walton	Cornerstone OnDemand	United Kingdom
Anette Westphal	Novo Nordisk A/S	Denmark
Christopher White	National Resilience, Inc.	USA

Regulatory Input and Review

Particular thanks go to the following for their review and comments on this Guide:

Arno Terhechte, GMP Inspector	Bezirksregierung Münster (District Gouvernement Münster)	Germany
-------------------------------	---	---------

Special Thanks

The Team Leads would like to give particular thanks to Mike Rutherford (Syneos Health, USA) for his efforts during the preparation of this Guide.

The Leads would also like to thank ISPE for technical writing and editing support by Jeanne Perez (ISPE Guidance Documents Technical Writer/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	7
1.1	GAMP Guidance	7
1.2	ISPE GAMP 5 Key Concepts	8
1.3	Overview	9
2	Critical Thinking for Computerized Systems	11
2.1	Introduction	11
2.2	Scope	13
2.3	Applying Critical Thinking	15
2.4	Practical Considerations	28
3	Adopting Agile Software Development in a GxP Environment	33
3.1	Introduction	33
3.2	Scope	36
3.3	The Discovery Mindset	37
3.4	From Requirements to Product	39
3.5	Tools Instead of Documents	46
3.6	DevOps, Continuous Integration/Deployment, and Product Teams	53
4	IT Service Management	55
4.1	Introduction	55
4.2	Scope	55
4.3	Accountabilities and Responsibilities of Regulated Companies and IT/IS Service Providers	56
4.4	Leveraging Supplier Effort	56
4.5	IT Service Quality Management	57
4.6	IT Service Models	64
4.7	Risk Considerations	67
4.8	IT/IS Service Provider Governance	69
4.9	IT/IS Service Provider Assessment	70
4.10	Management of IT Infrastructure	74
4.11	Validation of SaaS Applications, Demonstrating Fitness for Purpose	77
4.12	Managing Data in an Outsourced Environment (IT/IS Service Provider Support to Data Governance)	84
4.13	IT Service Operational Considerations	85
5	Appendix 1 – References	91
6	Appendix 2 – Glossary	95
6.1	Acronyms and Abbreviations	95
6.2	Definitions	97

1 Introduction

The ISPE GAMP® Community of Practice (CoP) [1] promotes the understanding of regulations and use of GxP computerized systems within the pharmaceutical, biopharmaceutical, medical device, and other regulated industries. *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems* [2] is the leading international guidance document in this area:

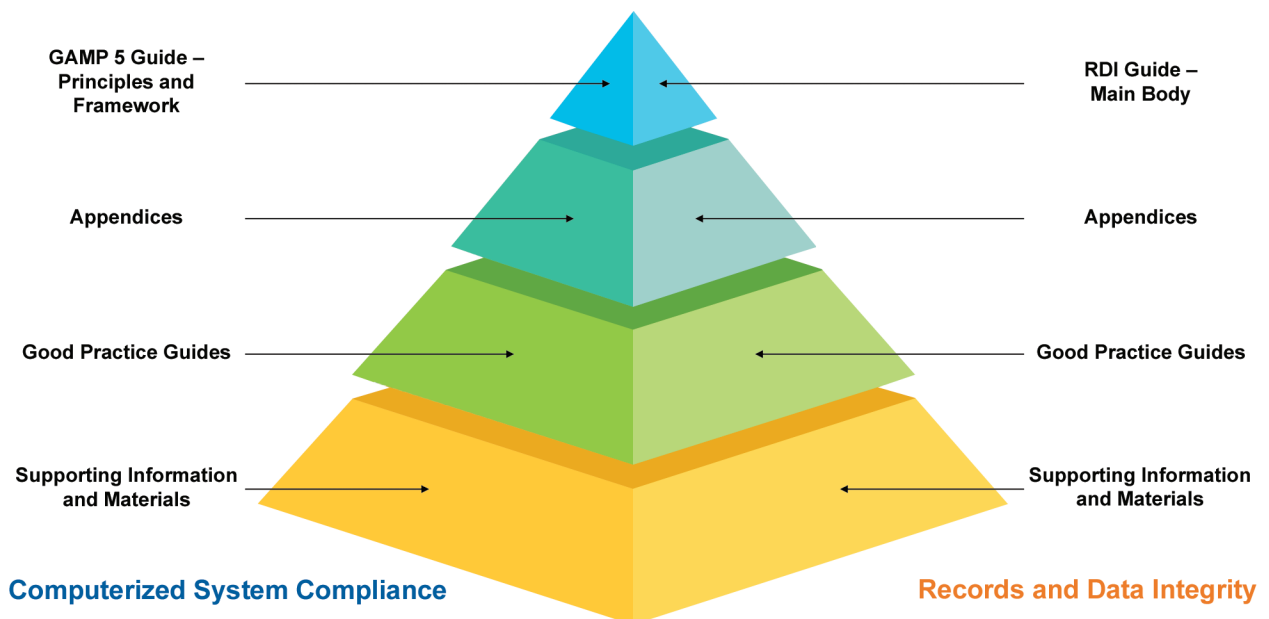
“GAMP® guidance aims to achieve computerized systems that are fit for intended use and meet current regulatory requirements, by building upon existing industry good practice in an efficient and effective manner” to safeguard patient safety, product quality, and data integrity.

This *ISPE GAMP Good Practice Guide: Enabling Innovation* discusses critical thinking, incremental and iterative (Agile) software development models and methods, and IT service management. By applying *ISPE GAMP 5* [2] principles and current good practice, the GAMP CoP seeks to enable life-science industry innovation and advancement in these areas. This *ISPE GAMP Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management* shows how these concepts are interwoven: applying critical thinking when leveraging software development practices, and using both concepts to effectively manage IT/IS service providers.

1.1 GAMP Guidance

This Guide is part of a family of guidance documents¹ that provide a comprehensive body of knowledge covering all aspects of GxP computerized systems good practice and compliance.

Figure 1.1: GAMP Documentation Structure



¹ For more information on the GAMP CoP and GAMP documentation, see www.ispe.org [3].

1.2 ISPE GAMP 5 Key Concepts

These five key concepts of *ISPE GAMP 5* [2] (also shown in Figure 1.2) form the basis of this Good Practice Guide:

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.”

2. Life cycle approach within a Quality Management System (QMS)

“Adopting a complete computerized system life cycle entails defining activities in a systematic way from system conception to retirement.”

3. Scalable life cycle activities

“Life cycle activities should be scaled according to system impact on patient safety, product quality, and data integrity, ...system complexity and novelty,” and supplier capability.

4. Science-based Quality Risk Management (QRM)

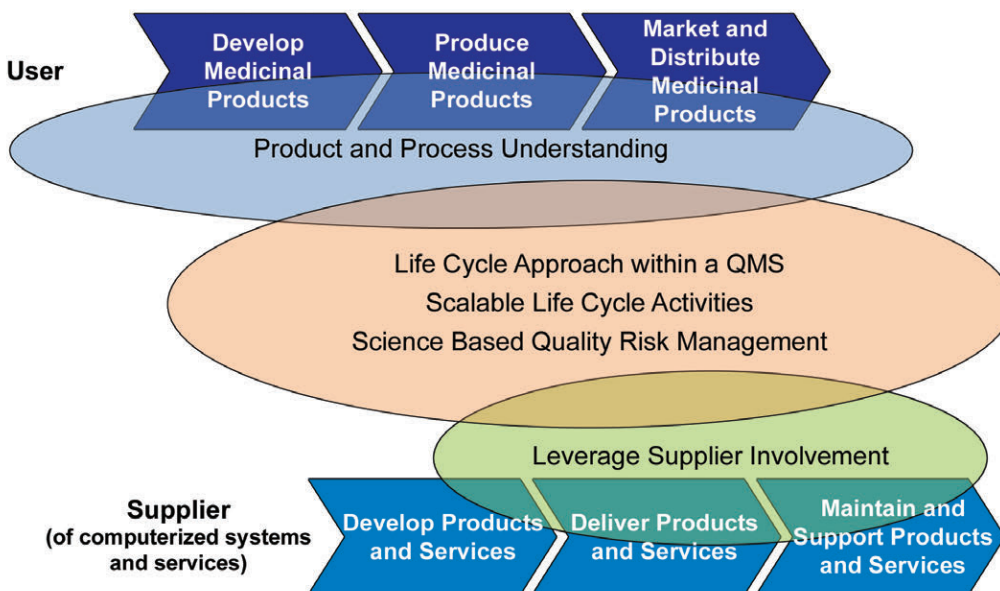
“Quality Risk Management is a systematic process for the assessment, control, communication, and review of risks.”

The *ISPE GAMP 5* QRM approach is aligned with ICH Q9 [4].

5. Leveraging supplier involvement

Regulated companies should seek to leverage supplier involvement and activities throughout the system life cycle while appropriately assessing and managing suppliers to minimize risks to patient safety, product quality, and data integrity.

Figure 1.2: ISPE GAMP 5 Guide Key Concepts [2]



1.3 Overview

This GAMP Good Practice Guide seeks to enable life-science industry innovation and advancement through the application of *ISPE GAMP 5* [2] principles and current good practice to the following key topic areas:

- The application of critical thinking
- Incremental and iterative (Agile) software development models and methods
- IT service management, including cloud computing

Chapter 2: Critical Thinking for Computerized Systems provides practical guidance on the adoption of a risk-based approach to the life cycle of GxP computerized systems based on critical thinking. It discusses how critical thinking may be applied to understand the intended use of the computerized system in the context of supporting GxP-business processes and the GxP data life cycle. Critical thinking supports the GxP principle of designing in quality (through system design, configuration, and operational controls) rather than the attempted testing in of quality.

Critical thinking allows the effective interpretation of data and situations while avoiding personal bias, inappropriate assumptions, and other distorting factors to retain rigor and balance.

As part of the Case for Quality program [5], the US FDA CDRH (Center for Devices and Radiological Health) has identified that an excessive focus on compliance rather than quality may divert resources and management attention toward meeting regulatory compliance requirements rather than adopting best quality practices. This may also deter investment in automation and digital technologies, which could assist in quality improvements and process control. An element of the FDA CDRH Case for Quality program is to promote a risk-based, product-quality and patient-centric approach to Computer Software Assurance (CSA). This encourages critical thinking based on product and process knowledge and QRM. [6] Chapter 2 discusses how critical thinking based on product and process knowledge and QRM can support such an approach. The application of critical thinking can enable the removal of barriers to the introduction of new and innovative technologies.

Chapter 3: Adopting Agile Software Development in a GxP Environment provides practical guidance on the adoption of iterative, incremental, or evolutionary (Agile) approaches to developing GxP computerized systems. Topics discussed include organizational culture, requirements management, specification and verification, and the use of effective tools and automation.

ISPE GAMP 5 [2] does not impose barriers to the adoption of iterative, incremental, and evolutionary approaches, and the specification and verification process described in it is not inherently linear. The FDA CDRH Case for Quality program [5] supports the adoption of Agile approaches where appropriate, in order to encourage innovation, eliminate unnecessary costs, and focus on quality and fitness for intended use.

Chapter 4: IT Service Management discusses good practices for assessing and managing IT/IS service providers. Regulated companies may utilize a diverse range of service models from IT/IS service providers to provide IT infrastructure, software, and data services. Delivery of these services range from traditional outsourcing models to Infrastructure, Platform, and Software “as a Service” (collectively referred to as XaaS or cloud computing). The appropriate implementation of cloud computing provides regulated companies with increased opportunities to adopt innovative methods to support the business. The application of these approaches requires careful consideration of the roles and responsibilities of the regulated company and the IT/IS service provider.

- **Accountability** entails ownership of the activity or task and being answerable if it is not completed correctly
- **Responsibility** entails doing what is necessary to ensure the activity or task will be completed correctly

Responsibility for IT-related activities may be delegated to IT/IS service providers, but in all cases regulatory accountability lies with the regulated company.

The regulated company must have defined roles and responsibilities for acceptance and release of GxP computerized systems. When outsourcing or delegating activities, there should be no resultant decrease in product quality, process control, or Quality Assurance (QA). There should be no increase in the overall risk of the GxP processes. The competence and reliability of service providers must be ensured.

Even though regulated companies cannot delegate their regulatory accountabilities to an IT/IS service provider, they may leverage the knowledge, experience, activities, and artifacts of an IT/IS service provider through risk-based assessment, management, and governance processes. A discussion of good practices in these areas is provided.

2 Critical Thinking for Computerized Systems

2.1 Introduction

Life cycle management of computerized systems in the pharmaceutical industry must ensure reliable operation and regulatory compliance while responding to the realities of maintaining and growing business profitability. While *ISPE GAMP 5* [2] presents a risk-based approach to ensuring fitness for intended use, some practitioners apply unthinking and rigid table-driven or tick-in-the box approaches not tailored or proportionate to the needs of different systems. Such suboptimal approaches often waste time and effort on non-value-added activities, leading to insufficient or excessive work with potential budget overspend and delays, and could inhibit innovation and the adoption of new technologies. Furthermore, these approaches may reduce focus on more valuable and essential QA activities.

The adoption of new and improved approaches to software engineering, data management, and “as a Service” offerings (XaaS), including the use of supporting tools, facilitate making the best use of resources and encourage the application of appropriate and proportionate practices. There have been schemes within the life sciences industries to improve processes that develop, manage, and maintain systems and software. Computer Software Assurance (CSA) within the US FDA CDRH Case for Quality program reinforces the importance of taking a risk-based approach that is primarily focused on impact to public health. [5]

This chapter discusses the concept of **critical thinking** applied to computerized systems. Critical thinking is defined in *ISPE GAMP® Guide: Records and Data Integrity* [7] as:

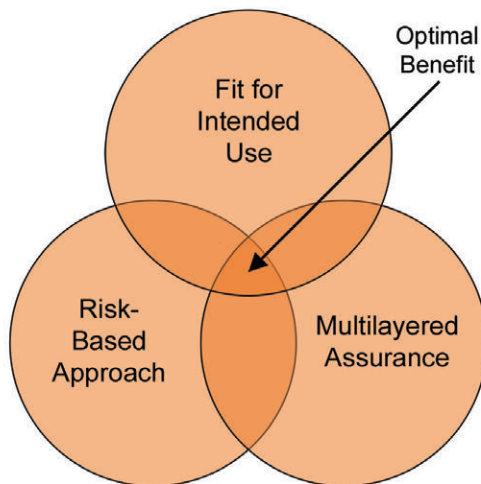
“a systematic, rational, and disciplined process of evaluating information from a variety of perspectives to yield a balanced and well-reasoned answer.”

Critical thinking allows the effective interpretation of data and situations while avoiding personal bias, inappropriate assumptions, and other distorting factors to retain rigor and balance. Critical thinking is aligned with the application of ICH Q9 Quality Risk Management [4] principles. Critical thinking is not just a tool for individual decision-making. It can and should become a habitual mindset based on an intellectual commitment of using those skills to guide behavior. [8]

Figure 2.1 illustrates critical thinking for computerized systems. The critical thinking mindset promotes the proactive adoption of a risk-based approach suitable for the intended use of the computerized system that takes into account the multiple layers of assurance provided by the business process. In other words, combining technical, procedural, and behavioral controls applied throughout the business process 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.

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. Business process mapping and data flow diagrams capture this information 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.

Critical thinking supports informed decision-making and good judgment on where and how to scale quality and compliance activities. The extent and depth of activities (and level of documentation formality – see Section 2.3.6) can, and should, vary to a considerable degree between different business processes, types of systems, functions within a system, and applications. It is here that significant efficiency improvements can be made by focusing on what is really needed and avoiding unnecessary work.

Figure 2.1: Critical Thinking for Computerized Systems

Critical thinking can bring benefits throughout the life cycle of a computerized system. The effectiveness of initial planning for a computerized system is dependent on the quality and extent of critical thinking applied. If the intended use of a computerized system is better understood, requirements and specifications are better defined, then the rigor of testing different aspects of the system will match the importance of the system functionality. If a supplier has demonstrably tested a software or system function, what is the real value proposition of repeating this test? Similar benefits can be found in the operation and maintenance of systems and management of data. Critical thinking is not a one-time activity and should be evident during the computerized system life cycle all the way through to retirement.

Regulatory authorities are adopting critical thinking to help them more quickly 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. Indeed, too much paperwork can confuse and make it harder to maintain and inspect computerized systems. Rather, 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 now offer the opportunity to demonstrate control in areas where separate documentation was previously considered a necessity, and these should be leveraged. [9] See Section 2.3.10 on inspection readiness.

Critical thinking involves questioning assumptions and eliminating bias. Bringing these into the risk-based approach can make the assessment process more objective. Critical thinking relies not just on basic knowledge of the business process but also on the detailed comprehension and analysis of where the business process can potentially impact patient safety, product quality, and data integrity. Critical thinking generates a better understanding of risks resulting in more confidence in the prioritization of those risks, and therefore supporting robust scaling of controls and validation activities based on that prioritization.

The combination of controls and validation activities provides multi-layered assurance. Critical thinking requires depth of understanding of the system within the context of the business process, such that the controls within the system complement the controls upstream and downstream in other systems to provide overall control. 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.

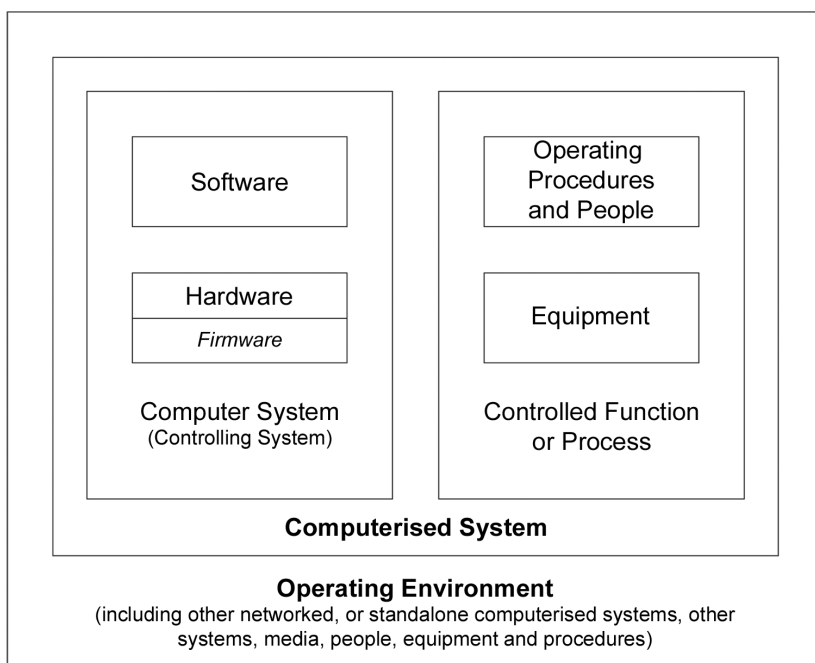
The benefits offered by critical thinking come from the experience and knowledge of the Subject Matter Experts (SMEs) specifying, testing, managing, and maintaining computerized systems. The SMEs can identify how best to realize the opportunities offered by critical thinking within a regulated company. The key objective is that computerized systems are fit for their intended use and efficiently maintained in a state of control.

2.2 Scope

A software application or computer system cannot be considered in isolation from its intended use, its role with the data life cycle of GxP data associated with the system, any connected ancillary equipment or interfaces, and its operating environment. This is defined in the PIC/S guidance Good Practices for Computerised Systems in Regulated “GxP” Environments [10] in 2007, as shown in Figure 2.2.

The definition of a computerized system is emphasized because a lack of precision in terminology may create confusion. Uses of the terms “application” or “computer” in place of computerized system does not limit the scope of computerized systems to software only. Software (i.e., the application) is only one component within a computerized system, which in turn is part of a wider operating environment. Failure to include all components of a computerized system in the scope of implementation, validation, and operational activities could result in not addressing potential risks to patient safety, product quality, or data integrity.

Figure 2.2: Components of a Computerized System [10]



2.2.1 Computerized Systems Life Cycle

A computerized systems life cycle approach means defining and performing activities in a systematic way from conception (understanding the requirements needed to support the intended use), through development, release, and operational use, to system retirement. The life cycle is scaled based on a risk-based approach with multiple layers of assurance to ensure the computerized system is fit for intended use. The project or development approach within the life cycle may be linear, iterative, or incremental.

Influences such as the increased adoption of Agile software development methods (see Chapter 3), Software as a Service (SaaS) application offerings and the associated software release cadence, and the need to update systems more frequently as part of cybersecurity efforts, mean there will increasingly be more changes during the operational phase of the life cycle. The effort needed to maintain the controlled, compliant, and validated state of the system through changes should not be a barrier to implementing upgrades so long as effective and efficient approaches are used.

Critical thinking combined with automated tools can facilitate efficient change management and regression testing. Automated test tools can verify critical functionality and ensure that regulated data is not adversely impacted after an application upgrade. Appropriate performance metrics can confirm solutions continue to be fit for intended use while safeguarding patient safety, product quality, and data integrity throughout the changes.

Chapter 4: IT Service Management discusses the advantages of moving from a fixed qualification approach for infrastructure to a continuous control and monitoring approach, which has the flexibility to accommodate and manage more frequent changes.

2.2.2 Data Life Cycle

A description of the data life cycle can be found in the *ISPE GAMP Guide: Records and Data Integrity* [7], and further discussed through three subsequent *ISPE GAMP RDI Good Practice Guides* [6, 11, 12].

Just as all components of a computerized system must be considered as part of fitness for intended use, so too must the aspects of the data life cycle that the computerized system supports. Each regulated record has an associated data life cycle where the data is created, processed, reviewed, reported and used, retained, and ultimately destroyed.

Note: Data and system life cycles operate on independent but related timelines. For example, a system may be retired before some of the most recent data within that system reaches the destruction phase of the data life cycle. This situation is discussed in Section 2.3.11.

Multiple systems may be involved in supporting a single data life cycle. For example, data may be created and processed in one system, reported and used to make GxP-decisions in an Enterprise Resource Planning (ERP) system, and then archived for the retention period in another. A data flow diagram derived from business process mapping illustrates all of these and helps to identify the regulated-data life cycle.

Areas to apply critical thinking to the data life cycle include, but are not limited to:

- Assessing the regulated-data life cycle holistically, considering all the systems and the interfaces between them that have the potential to impact the integrity of the GxP data
- Ensuring the system's user requirements reflect the technical controls required for the specific stages of the data life cycle that the system will support. For example, an archive system only supports the retention phase of the data life cycle, and therefore does not require controls for creating and processing data.
- Identifying what data needs to be archived and how to transfer that data if the archival solution is not the original system
- Understanding the diminishing value of data as it moves through the retention period and how that impacts the controls required
- Planning the means to view archived data if the original system that created the data is decommissioned

Mergers, acquisitions, and divestments can change data ownership and disrupt the data life cycle. Practical considerations for this are discussed in Section 3.7 of the *ISPE GAMP® RDI Good Practice Guide: Data Integrity by Design* [6].

2.3 Applying Critical Thinking

2.3.1 Risk Management

QRM, as defined in ICH Q9 [4] and adopted by *ISPE GAMP 5* [2], is:

“a systematic process for the assessment, control, communication, and review of risks”

It is an iterative process used in the computerized system life cycle from concept to retirement. The objective of QRM is to identify risks to patient safety, product quality, and data integrity, and to apply appropriate controls to reduce those risks to an acceptable level.

Applying critical thinking to the risk-management process enables organizations to appropriately scale data and system life cycle activities and controls.

Figure 2.3: *ISPE GAMP 5* Quality Risk Management Process [2]

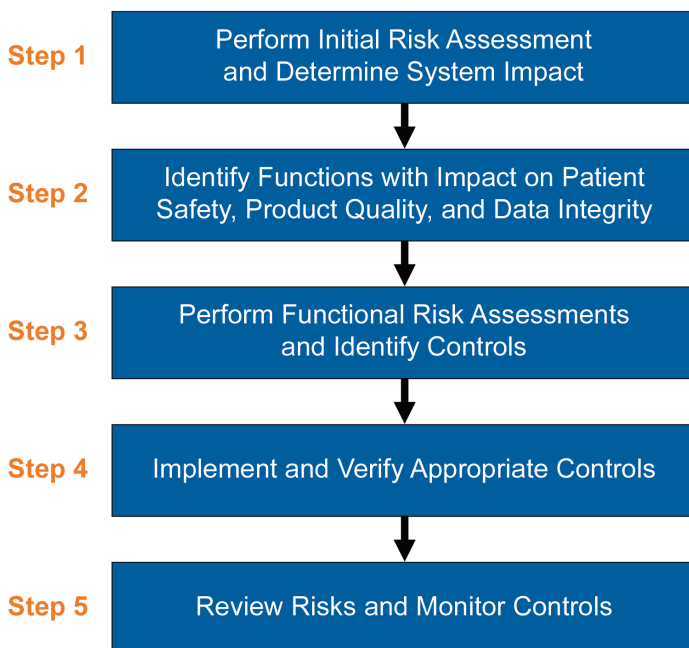


Figure 2.3 depicts the QRM Process described in *ISPE GAMP 5* [2]. Many organizations have focused on applying Step 3 of this process (the functional risk assessment that derives an overall risk priority based on severity, probability, and detectability) to all system functions without first adequately addressing Steps 1 and 2, and without applying critical thinking.

Step 1 provides the decision whether to proceed to Step 2 based on the overall impact that the computerized system may have on patient safety, product quality, and data integrity due to its role within the business processes.

Step 2 refines the scope of future activities based on which functions/features have an impact on patient safety, product quality, and data integrity. Functions not having an impact do not need to feed into Step 3.

Step 3 is the functional risk assessment that includes only those functions having an impact on patient safety, product quality, and data integrity. Functions identified in Step 2 should be assessed by considering possible hazards and how the potential harm arising from these hazards may be controlled. Understanding of the potential impact is aided by defining the business process and data flows, and assessing risk based on the overall business process, not just on an individual step in a system. Critical thinking should be applied to ensure the assessments are as effective as possible. For example, by assessing at a modular level, then at a business process level, and then at a functional level.

When assigning a rating for severity of harm to a potential failure, it is important to consider the overall risk of the system at the business process level. A complete failure to meet a requirement may render part of the system nonfunctional, but in a system with low overall risk to GxP, it probably does not rate as a high severity of harm with respect to patient safety, product quality, and data integrity. There could, however, be justification for classifying severity of harm as high with respect to its impact on the organization's other operating imperatives.

Similar requirements relating to a specific area of functionality may be grouped together in a recursive hierarchy consisting of major requirements and subsidiary requirements. This hierarchical approach, which may have multiple levels depending on the complexity of the process or system, may help simplify requirements management and risk assessment. Major requirements² are assessed based on severity, probability, and detectability to derive an overall risk priority (High, Medium, or Low per *ISPE GAMP 5* Appendix M3 Figure M3.5 [2]).

Critical thinking and the major requirement risk priority (e.g., is it high risk?) should determine whether some or all of the more detailed subsidiary requirements need to be individually assessed within the hierarchy of functionality. A subsidiary requirement cannot have a risk priority higher than that of the major requirement, so there may be no benefit to assessing subsidiary requirements of a low-risk priority major requirement. However, for a higher-risk major requirement, identifying subsidiary requirements with lower-risk priority prevents the need to automatically test all subsidiary requirements. Combining this approach with a testing strategy based on increasing test rigor and documentation with increasing risk priority ultimately results in efficiency gains.

Assessing the risk at the major and/or subsidiary level as needed ensures the selection of optimal control measures (configuration settings, procedural controls, data review processes, etc.), and testing rigor and documentation, commensurate with the assigned risk priority.

Risk assessment allows the identification of appropriate behavioral, procedural, or technical controls to reduce risk to an acceptable level. They may be part of a computerized system function, or in parallel manual procedures, and may be upstream or downstream of the system. Controls typically are aimed at:

- Eliminating risk through process or system redesign
- Reducing risk by reducing the probability of a failure occurring
- Reducing risk by increasing the in-process detectability of a failure
- Reducing risk by establishing downstream checks or error traps (e.g., fail-safe, or controlled fail state)

The risk priority may be used as input to decisions on rigor and extent of controls. For example, application timeout and password complexity are both controls to reduce the risk of unauthorized access to a system. The duration of the timeout and the extent of password complexity may be influenced by the risk priority, with shorter timeouts and greater complexity where the risk has been assessed as high.

Step 4 implements and verifies the controls selected in Step 3 to ensure that they have been successfully implemented. Controls should be traceable to the relevant identified risks. The verification activity should demonstrate that the controls are effective in performing the required risk reduction.

² See Section 2.3.3 for examples of major and subsidiary requirements.

Some companies have a policy at the organizational level that provides guidance on the test strategies applicable to the different controls and risk priorities. Critical thinking can assess the supplier testing completed on the identified controls and determine what, if any, additional assurance is needed and what assurance approach(es) (or combination of approaches, e.g., ad hoc, exploratory, robust scripted etc.) is most appropriate based on the risk priority assigned in Step 3. Determining the appropriate assurance approach is discussed in detail in Section 2.3.7.

Step 5 is performing system periodic review or planning changes to the system. Critical thinking should be applied to evaluate trends in performance metrics, changes in the assessed risks, the impact of changes in the system, the need for changes to the implemented controls, and the need for new or regression testing activities.

It is not necessary to apply the steps in this risk-management process for nonregulated systems, although there could be other business reasons to do so, such as if the system is critical to the ongoing operation and the organization wants to benefit from the risk-based approach in all areas.

The level of effort, formality, and documentation of the quality risk-management process should be commensurate with the level of risk. The effort involved in applying the risk-based approach should not be more burdensome than if it were not applied. Key stakeholders for risk assessments include IT, quality, the process owner, and SMEs skilled in computerized system validation, risk management, and critical thinking.

2.3.2 Planning

In order for an organization to implement a computerized system that supports their business process and ensures data integrity, they should use a holistic approach. Planning for individual systems is discussed in *ISPE GAMP 5* Section 4.2.1 [2].

A business process is often supported by multiple computerized systems. An organization may aim to improve the efficiency, data integrity, or regulatory compliance of the business process by looking to update one of the systems or consolidate multiple systems into a single enterprise system. Critical thinking must be applied throughout the process to understand the risks to patient safety, product quality, and data integrity, and in particular, for an understanding of the effect and risks of the implementation of the new computerized system.

To facilitate effective system planning, it is important to understand the business process and the data flow, including all regulatory requirements. Developing business process maps and data flow diagrams to illustrate business activities is described in *ISPE GAMP Guide: Records and Data Integrity* [7] and the *ISPE GAMP RDI Good Practice Guide: Data Integrity by Design* [6]. A full understanding of the regulated process to be supported, including the intended use of data within the process, is fundamental.

The business process flowcharts illustrate the business activities, decision points, and subprocesses, while the data flow diagrams identify the creation, movement, use, and archiving of data. Together these diagrams help in the understanding of the business process to identify risks to patient safety, product quality, and data integrity associated with the process. Data integrity cannot be achieved without a complete understanding of the data flow.

Examples of planning using critical thinking include:

- Utilizing business process mapping and data flow diagrams to understand where the computerized system will fit in the process, what regulated data will pass through it, and what part of the regulated data's life cycle the system will support
- Defining consistent nomenclature for use in the process to facilitate data transfer, trending, and analytics
- Selecting a solution that best fits the business requirements minimizing configuration and customization, recognizing that it may be more pragmatic to adjust the business process to fit a standard application

- Understanding the interfaces needed to other systems, and what standard interfaces are available versus developing new interfaces (with their additional test and management burden)
- Planning for how the system should behave during normal operation as well as how it should respond in an error or failure situation and how it can recover from such a situation

2.3.3 Requirements

The key to the implementation of a computerized system fit for intended use is to thoroughly understand the business process and data requirements to enable the creation of user requirements. Not all requirements need to be finalized before proceeding (for further information on Agile approaches see Chapter 3). Requirements should define the functionality required to support the business process as well as ensure compliance with applicable regulations, for example, data integrity. Guidance on defining data integrity requirements is contained in *ISPE GAMP Guide: Records and Data Integrity* [7] and *ISPE GAMP® RDI Good Practice Guide: Data Integrity – Key Concepts* [11].

Critical thinking should ensure that requirements specifically relating to regulatory compliance are tailored to the system's intended use rather than indiscriminately applying every potentially applicable regulatory reference when some are not appropriate or necessary. For example, following the text of the regulation for an audit trail requirement can result in oversized tables of text entries that are dependent upon manual review. Applying critical thinking initially evaluates whether a data audit trail is appropriate or necessary, in other words, are users expected to create, modify, or delete regulated records during normal operation? If an audit trail is required, critical thinking should be used to develop requirements (including Agile user stories) for an audit trail that is contextual, searchable, filterable, and reportable. In this way, critical thinking enables the development of more efficient and effective controls.

Increasing levels of requirements granularity can be expressed and managed by using a recursive hierarchy within the specification. In the example above, the major requirement would be:

- The system must have a time-stamped, computer-generated audit trail

The subsidiary requirements then describe how to ensure effective and efficient controls. Some simple examples to illustrate this hierarchical approach are:

- The audit trail will record operator entries and actions that create, modify, or delete regulated data (e.g., within the batch record).
- The audit trail shall be searchable by any of the recorded information, e.g., user ID, description, date, time.
- An exception report can be generated from the audit trail, checking for user-defined criteria.

The subsidiary requirements may not necessarily be specifically defined in the regulations but may significantly impact the usability of the system. As noted in Section 2.3.1, critical thinking may warrant the risk assessment of individual subsidiary requirements of a high risk major requirement to better scale the controls and the testing effort.

Developing defined requirements is an essential precursor to identifying those with the potential to impact patient safety, product quality, and data integrity, and to applying QRM approaches, as discussed in Section 2.3.1.

2.3.4 Supplier Assessment and Selection

By performing assessment, management, and governance activities, regulated companies should ensure that suppliers, including service providers, will meet the regulated company's technical, business process, and regulatory requirements. Confidence that a supplier offering will support the business process needs to be based on assessing their capability for developing, implementing, and maintaining a system fit for the regulated company's intended use. In the case of "as a Service" offerings, this should include assurance of the long-term provision and stability of that offering. The need for supplier audits (initial and ongoing) should be based on risk. Supplier assessments should determine whether the supplier is suitable for use.

Knowledge of the processes followed by the supplier can enable the regulated company to reduce their validation effort by leveraging supplier activities, as described in *ISPE GAMP 5* [2] and *ISPE GAMP RDI Good Practice Guide: Data Integrity – Key Concepts* [11].

Critical thinking combined with a clear understanding of the business process enables evaluation of the computerized system's functionality and the supplier's specifications. Rather than just noting the presence of a development life cycle during a supplier assessment, applying critical thinking during the assessment establishes the transparency and traceability of the supplier's internal development life cycle to determine how much of the supplier activities can be leveraged. This may require participation from the regulated company's business process owner, compliance, and technical experts during the assessment. Further discussion of how critical thinking can be applied to reduce user validation of Commercial off-the-Shelf (COTS) products has been published elsewhere [13].

It is important to understand the origin of the supplier's software modules and libraries. It is becoming common to request a *Software Bill of Materials* to understand the various components and any use of Open-Source Software (OSS).

Dependence on, and trust in, a supplier is not based on a single assessment but rather aggregated throughout the system life cycle and includes reassessments. Critical thinking should ensure that supplier selection criteria contain performance measures such as system reliability, service continuity, and reputation for customer responsiveness. For certain types of system architecture, such as SaaS, reliance on the supplier may not be limited to the system life cycle and can include the data life cycle, which should be assessed during service provider selection.

2.3.5 Impact of Supplier on Regulated Companies

Maximizing efficiency between suppliers and regulated companies requires critical thinking from both parties, even when the supplier is in-house to the regulated company.

Where a supplier is creating an offering to the life sciences industry (whether that be a control system element such as a Programmable Logic Controller (PLC), analytical laboratory equipment, IT software solutions, or a SaaS application), it will have its own life cycle where it is planned, specified, implemented, verified, and reported as fit for intended use as part of an internal release process. A supplier's offering may be used by a regulated company as is, parameterized, configured, or customized to meet the requirements of the business process.

The supplier should apply a risk-based approach to their development life cycle, including their test strategy. Supplier activities should focus on ensuring their product meets their specifications by effective and efficient means; however, there will be a minimum level of detailed information and evidence of effective testing expected by a regulated company. For example, critical thinking would identify that ineffective testing approaches instead of robust and/or automated testing may reduce the opportunity for the regulated company to leverage the supplier's activities. Where the supplier has used a risk-based approach, the regulated company should determine if their assessment of risks is different to that of the supplier and adjust accordingly.

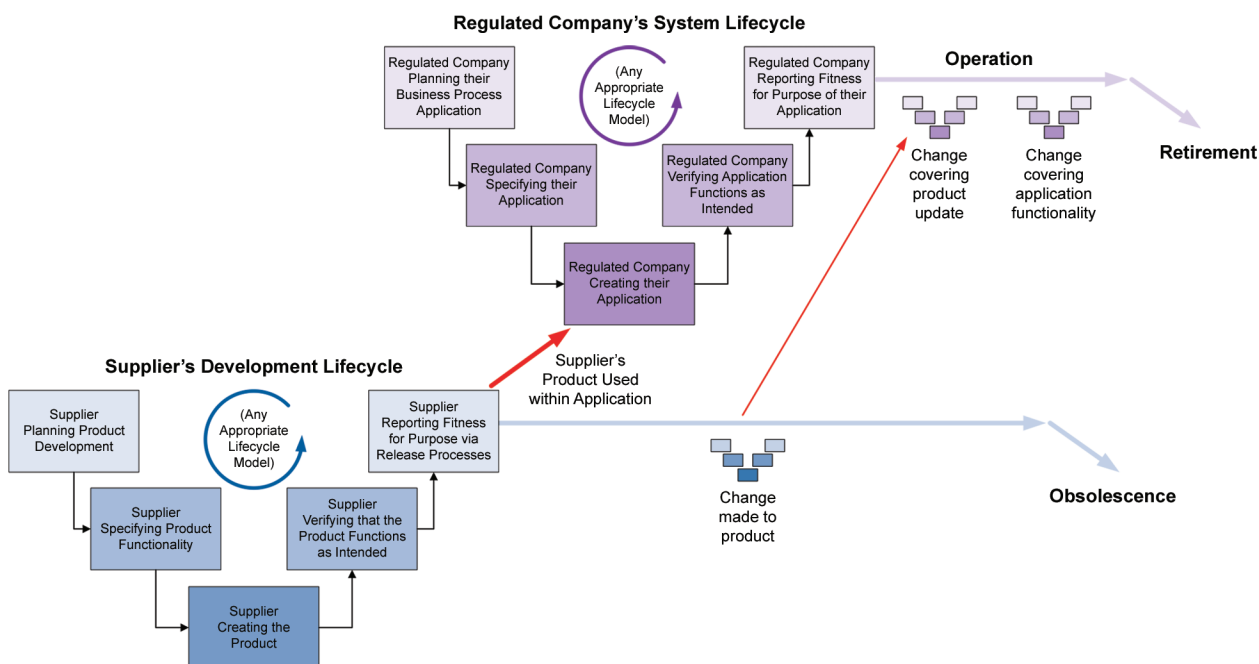
The better the quality of the supplier's development processes (e.g., supplier's **development** life cycle), the more efficient the regulated company's implementation of the supplier's offering can be (regulated company's **system** life cycle), as depicted in Figure 2.4.

Neither of these life cycles are a single event. The supplier will release updates to their products and services, and the regulated company will need to assess the updates and, if implementing them, use operational change control to apply the updates. Where a regulated company has in some way customized the offering, the effort to implement the update may be proportionally larger.

In an “as a Service” offering, particularly multitenant SaaS applications, the use of a DevOps approach³ can result in more frequent changes with little or no opportunity for the regulated company to assess or reject a change. It is inherent to the service model that the development life cycle may drive the validation schedule and change control. Managing and leveraging service providers is discussed in more detail in Chapter 4.

Figure 2.4: Interaction of Supplier and Regulated Company Life Cycles

Adapted from ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition) [14]



Critical thinking should be applied to ensure that:

- The supplier's understanding of how their product is used in the life sciences industry allows them to specify and test their product in a way commensurate with its potential risk to patient safety, product quality, and data integrity.
- Regulated companies are accountable for ensuring the system is fit for intended use, and should evaluate the supplier's approach against the regulated company's intended use. Access to supporting information around supplier activities should be defined in the purchase contract or Service Level Agreement (SLA).
- Regulated companies should leverage the supplier's information describing the functionality of the product so that they can cross reference to their own requirements. This enables the regulated company to analyze the functionality and identify any areas that need configuration or customization to suit their business process. They should also seek to leverage the activities performed by the supplier.
- Information and test evidence in the form of artifacts within requirements management tools and automated test tools are given equal credence with discrete formal documentation. Further considerations for the use of tools are discussed in Section 2.4.4.1.
- If the supplier's system is to be interfaced to other systems within the regulated company, for example LDAP (Lightweight Directory Access Protocol) authentication or single sign-on, the interfaces need to be defined, implemented, validated, managed, and maintained.

³ A DevOps approach combines software development and system operations and is often used to support continuous delivery.

- Where feasible, the supplier should aim to develop customer-requested new functionality into their mainstream product offering rather than creating special versions for individual customers. This reduces the supplier's product management effort and simplifies future updates for all parties. If the functionality is provided as a configurable option, there is no obligation on other customers to implement it.
- Where a regulated company requests the development of a new or amended feature, keeping it within the supplier's development life cycle ensures it is done once and tested once rather than developed and tested repeatedly by regulated companies.
- Reuse of standard modules of code or custom-developed forms, by the supplier or regulated company, should be based on a master template to ensure changes are automatically replicated across all instances. This reduces the possibilities of errors (e.g., introduced by copying and pasting for reuse), condenses the need for testing to just the master template, and eliminates the possibility of one or more instances not being updated.
- Ongoing management and implementation of changes is done in a controlled way by:
 - Leveraging supplier activities and knowledge (i.e., in the same way as that for the original development).
 - Ensuring changes to the product can be communicated to the regulated company so they can assess the risks of taking or not taking the change. (Note that in some offerings the change is not optional for the regulated company, e.g., multitenant SaaS).
 - Having a pre-verified method for installing the change. The regulated company should apply critical thinking around the risks of taking versus not taking the change, assessing likely risks to their intended use as a result of the change, and leveraging what has been done by the supplier in order to install the changes with the minimum of repeated effort.
- Where a supplier is involved within the regulated company's life cycle (e.g., a systems integrator), the supplier and regulated company should jointly agree on the overall rigor of documentation and testing required and who will be responsible for which elements in order to avoid unnecessary duplication.

2.3.6 Plans, Specifications, and Reports

The specification and verification approach described in *ISPE GAMP 5* [2] for project phase activities has been interpreted as a linear-sequential approach. In fact, the model is not confined to linear-sequential approaches and has much greater value as a relationship diagram. Irrespective of the software development process followed and the validation strategies adopted, the key objectives of the project phase of the system life cycle are that the verification activities are traceable to the system specifications, and the reporting stage identifies compliance or noncompliance to the system requirements and validation plans.

ISPE GAMP 5 [2] and *ISPE GAMP Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [14] provide detailed guidance on testing strategies and documentation. *ISPE GAMP 5* states that the supplier's specifications and test evidence should be assessed for suitability, accuracy, and completeness. It specifically states that "*there should be flexibility regarding acceptable format, structure, and documentation practices*" as there is no value in recreating documentation in a different template.

Critical thinking can be used to determine:

- Scaling activities and records based on risk
- If the supplier's specifications and evidence are adequate for leveraging to support the regulated company's system life cycle, and available when needed
- What information needs to be directly available at the regulated company versus referencing the supplier's records

- Who should be the vital few reviewers/approvers and in what context are they reviewing/approving. In practice, having more approvals usually leads to lower quality and value as everyone thinks someone else has looked at the detail. Segregation of duties must be preserved where required.

The application of risk-management approaches determines the areas of highest risk within the computerized system. Critical thinking then enables tailoring the level of formality for test plans and specifications for the highest risk areas. For example, not all testing records have to be to the same level of detail. The use of critical thinking for testing is covered in Section 2.3.7, and the use of tools is discussed in Section 2.4.4.

2.3.7 Testing

A key principle from testing theory is that exhaustive testing is impossible [15], and consequently testing can only show the presence of defects and cannot prove the absence of defects. Early and efficient testing, during development as well as during the verification phase, improves defect detection and reduces the occurrence of defects surviving into the operational phase.

Risk-based approaches focus test effort on high-risk functions and inherently do not test everything; therefore, there is the possibility that some defects will not be detected. Regulated companies should apply critical thinking when investigating escaped defects discovered in the operational phase. An excessive response may be to initiate a test all approach to find other escaped defects. Instead, test metrics should be used to confirm that the actual escape rate of defects is in line with the assumptions made when determining the type of testing to be carried out for functions and features with different risk priorities. An unacceptable number of escaped defects in high-risk functions requires re-evaluating the functional risks and the corresponding test strategies.

Another concept from testing theory is the Pesticide Paradox⁴ [16] whereby based on the results of testing, programmers improve their programming practices (i.e., fix the defects) so as to make previous test cases ineffectual at defect detection.

In order to avoid test specification deviations, testers often dry run protocols to ensure they will run without test script errors during the formal execution because the consequences of a test scripting/authoring error are disproportionately high. The test cases are run until they have little possibility of detecting a defect, providing no value from a testing perspective. This focus on error-free test scripts takes time away from testing without benefit to patient safety, product quality, or data integrity.

Regulated companies should think critically on strategies to minimize the bureaucracy associated with correcting largely inconsequential script errors so that the dry run activity can be minimized. Errors that impact product quality will trigger detailed investigations compared to a *catch and correct in the moment* approach for less significant typographical errors. Testing techniques such as unscripted and ad hoc testing (discussed in Section 2.4.4.2) can dramatically reduce the incidence of script errors, although depending on risk priority, a level of scripted testing may still be required. Unscripted testers should be qualified as testers and trained, competent users of the system to ensure the testing is focused on challenging the application in the context of the business process. Test activities should be traceable to the requirements.

2.3.7.1 Approach

ISPE GAMP Guidance [17] promotes a risk-based approach to GxP computerized systems compliance and fitness for intended use. The FDA CDRH Case for Quality program [5] reinforces the need to take a risk-based approach to testing and to focus testing effort on functions or features that present risk to patient safety, product quality, and data integrity while using critical thinking to ensure efficient test approaches.

⁴ The Pesticide Paradox – If the same tests are repeated over and over again, eventually these tests no longer find any new defects. To detect new defects, existing tests and test data may need changing, and new tests may need to be written. Tests are no longer effective at finding defects, just as pesticides are no longer effective at killing insects after a while. In some cases, such as automated regression testing, the pesticide paradox has a beneficial outcome, which is the relatively low number of regression defects. [16]

A combination of direct evidence (e.g., manual or automatic recording of results, screenshots) and indirect evidence (e.g., reports, notifications that can only exist if the proving step is completed) can be used to establish that requirements have been fulfilled in support of the intended use.

By applying critical thinking throughout the life cycle (see the other subsections within Section 2.3), the functions and features to be tested can be defined with appropriate risk priorities applied that reflect:

- The potential impact on patient safety, product quality, and data integrity (high priority functions with the greatest risk require greater test rigor and level of documentation detail)
- Prior testing of the function or feature either in the supplier's development life cycle or as part of the regulated company life cycle. Automated tools within the supplier's development life cycle may have enabled and included full regression testing of daily builds.
- The degree of confidence in that prior testing based on supplier assessment

Using critical thinking, those risk priorities can then be used as input to determine the appropriate test approaches. The aim of testing is to identify and allow the removal of defects and confirm fitness for intended use rather than producing documentation for documentation's sake. Critical thinking can optimize test approaches for the regulated company such as:

- Planning and organizing tests to run as efficiently as possible, for example by combining tests to minimize repeated test setup activities, and/or by grouping related functionality testing
- Ensuring sufficient test coverage during the system life cycle, with the rigor of testing commensurate with the assigned risk priority, and avoiding repeating tests that are similar or identical to those carried out by others
- Ensuring that the test cases demonstrate that functions operate correctly
- Differentiating between proving steps and non-proving steps to limit the amount of test execution evidence created and retained. Proving steps demonstrate a requirement has been fulfilled, while non-proving steps are used to set up the proving step. This ensures test evidence is only captured for proving steps that demonstrate a higher-risk GxP or business requirement has been fulfilled.
- Making test cases specific and unambiguous such that a reviewer can objectively determine if the test passed or not without subjective analysis or excessive evidence (see Section 2.3.7.2)
- Ensuring the testers have the skills and expertise to execute the tests, operate the system, and evaluate the results in the context of the intended use and/or the business process. This then obviates the need for overly prescriptive and detailed test instructions and in turn reduces test incidents arising from poorly written test scripts.
- Minimizing pressure on testers, e.g., to meet a deadline for moving to the operational phase, which can bias testing outcomes
- Enabling a proportionate review of completed tests based on the risk priority of the function under test
- Leveraging automated test tools and test management tools in place of extensive manual effort and referring to the test artifacts within the tools in place of documentation (see Section 2.3.7.2 for examples of reducing test effort by using automated testing, and of reducing test results documentation by leveraging the audit trail entries generated during automated testing)
- Managing incidents and their corrective actions to ensure any changes are fully verified once completed, including an appropriate amount of regression testing to ensure that the change has not adversely affected other functionality

Test strategies should ensure sufficient system testing to detect defects, and that test management processes are robust enough to maintain control of the system during the testing activities. Some possible strategies for scaling test rigor and documentation in the regulated company's system life cycle are discussed in greater detail in *ISPE GAMP RDI Good Practice Guide: Data Integrity by Design* Appendix S2 – Computer Software Assurance [6].

The critical thinking rationale behind the test strategy must be documented.

2.3.7.2 Test Evidence

Testing activities and test evidence should focus on demonstrating fitness for intended use by showing that quality-critical requirements have been met, identifying defects so they may be removed, and ensuring that risk-management controls are effective.

A combination of test approaches (such as exploratory, error guessing, manual/automated, unscripted and scripted testing) is needed at various stages in the system life cycle in order to achieve these objectives. The test evidence or output varies from case to case and depends on the detailed testing technique and intended readership.

The organizational policy, or the test specification itself, should define the requirements for test evidence, including the recording and reporting of test pass/fail results. *ISPE GAMP 5* Section 8.5.3 [2] identifies excessive and unnecessary hard copy test evidence as an area for efficiency improvement. In particular, it acknowledges the significant overhead associated with hard copy evidence and reiterates the need for a:

“justified and documented decision, based on impact, novelty, and complexity” of the system.

In many cases, additional hard copy evidence such as screen shots do not add value and are unnecessary.

The objective evidence for the testing performed may include the application data and objects created during testing and can leverage the system audit trail, if it has been verified to accurately capture input, transactions, and outcomes in sufficient detail. The audit trail also enables the company to generate and retain further detailed test evidence when using unscripted testing techniques. Supplemental evidence (e.g., reports, screenshots) can be captured when it adds value beyond the audit trail, for example, investigating errors, facilitating the ease of review, documenting the complexity of the transaction.

Test evidence is inherent in the application data and audit trail entries created during testing (documented unscripted testing is discussed in Section 2.4.4.2), which can be reviewed as required. Additionally, the system's previously verified functionality can be demonstrated as fit for intended use within the test environment or production environment as applicable.

Critical thinking around applying a risk-based approach to the extent of test evidence supports:

- Ensuring that even where testing is not scripted in detail, the objective of the test remains clear, and the results record adequately what testing was carried out. (Unscripted does not mean undocumented – see Section 2.4.4.2.) Evidence of a test case result can be as straightforward as the tester indicating if a test passed or failed.
- Ensuring that test evidence is only collected for proving steps that are not inherently covered by evidence from another test.
- Adopting an exception-reporting approach to recording detailed results. That is, that if the system response matches the expected results, a simple “Pass” can be recorded. However, if the system responds in an unexpected manner, the tester records both a “Fail” and a description of how the response differed from the expected results, as this additional detail is helpful in determining the root cause and corrective action. This eliminates time wasted capturing elaborate test evidence (e.g., excessive screenshots or recording detailed descriptions of the observed response) when a simple pass or fail (or recording the value or initialing a design specification statement) is adequate to confirm that the test has been completed.



- Recognizing that screenshots as objective evidence may now be considered as bringing little value to verification activities. Note that there are a number of situations explained in the *ISPE Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems (Second Edition)* [14] where they offer a practical benefit over manual recording when detail is needed, e.g., when there is a specific need for a before and after comparison of detailed or complex data, such as an audit trail or report.
- Acknowledging that it is disproportionate and unnecessary to use test witnessing or requiring the tester to initial every test step to affirm they followed the instructions
- Encouraging the use of automated testing tools to minimize manual collection of evidence as the artifacts within the tools are themselves evidence

2.3.7.3 Reviewing Completed Testing

Completed testing should be reviewed to verify that the computerized system is fit for its intended use. Test evidence should be reviewed to confirm completeness and accuracy of conclusions.

There is little value in:

- Looking for minor errors in documentation that have no impact on patient safety, product quality, or data integrity
- Forensically scrutinizing test evidence to assess whether the tester has exactly followed the test instructions for non-critical functionality

Unusual patterns of test failures associated with particular authors and/or individual testers should be investigated to determine whether there are any wider testing implications on the rigor of completed testing.

2.3.8 Operation and Maintenance

The operational compliance of a computerized system – and hence the safeguarding of patient safety, product quality, and data integrity by that system – is significantly impacted by the working practices of its users. Critical thinking and user consultation across both the business users and the IT support group Standard Operating Procedures (SOPs) should be applied to develop a framework of easily understood and intuitive practical instructions (e.g., SOPs, video how-to guides, built-in online help) for routine use and data review, system support, incident management, and system administration, etc.

The configuration choices and controls implemented during the project phase will only be realistically exercised during the use of the system. Such controls should be reviewed, often in periodic review (discussed in Section 2.3.9), using critical thinking to assess whether they are truly mitigating the risks as intended, and whether they still enable efficient business operation. Changes to system configuration are typically captured into a system audit trail that should be regularly reviewed to ensure no unauthorized changes have been implemented.

Detailed information about how to maintain computerized systems throughout their operational phase is discussed within *ISPE GAMP 5* [2] and *ISPE GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [18].

Since those guides were published, changes in technologies and development methods have led to an increase in release cadence for applications. The regulatory expectation is that application updates that offer improvements to patient safety, product quality, or data integrity should be applied when available and that GxP systems do not run on unsupported operating systems. [9]

This requires regulated companies to implement operational controls as a flexible and streamlined process, leveraging critical thinking and risk-based approaches, to manage and maintain the system and its compliant use through ongoing changes and evolution during its operational life. This allows change to be embraced in support of improved operation rather than avoided as long as possible because of the perceived validation and documentation burden associated with change.

Increasing incidences of cyberattacks have forced the industry to routinely adopt patches and hotfixes immediately after release to address potential security vulnerabilities. Managing IT infrastructure changes proficiently is addressed in Chapter 4.

When a system has been tested using a risk-based approach, it is inherent that a residual level of risk has been accepted including the possibility that there may be defects, particularly in low-risk functionality, that were found during testing and are still present in the system. When a defect is discovered during operational use and the incident management process triggered, it is important to apply critical thinking during the root cause analysis to assess whether the original risk-based testing approach is still valid. This is discussed in Section 2.3.7.

2.3.9 Periodic Review

During periodic review the system is assessed for the cumulative impact of any changes, defects, or regulatory updates. The frequency of periodic review should be based on the GxP impact of the system, with high-risk systems reviewed more frequently. Critical thinking should be used to determine whether the review frequency should be increased or decreased based on the outcome of the previous review and/or performance trends. For example, if issues and failures were found during the last periodic review, the review period can be shortened to make sure the Corrective and Preventive Actions (CAPAs) were completed and have resolved those issues.

Additionally, periodic reviews may be triggered by other processes such as performance monitoring, incident management, and CAPA. Periodic reviews will be needed more frequently if the system is not managed using performance monitoring metrics. Critical thinking should also be used in conjunction with system performance metrics and trending data to identify areas for improvement within the system's use, maintenance, and ongoing operation. This includes considering whether incremental changes to the system's functionality has extended the system beyond its intended use.

Critical thinking can be applied to ensure that the appropriate rigor is applied to change management to minimize the frequency of periodic reviews and ensure the validated state is maintained, thus eliminating the need for revalidation.

Periodic review is referred to in Section 2.3.1 and is more extensively discussed in the *ISPE GAMP Good Practice Guide: A Risk-Based Approach to Operation GxP Computerized Systems* [18].

2.3.10 Inspection Readiness

Having applied critical thinking, it is vital that this thinking and the subsequent approach taken to various aspects of the life cycle of a computerized system are evident for regulatory inspection. Policies and procedures can position where critical thinking will be applied, and plans and specifications prompt specific considerations during its application. The practical application of critical thinking, however, also needs to be evident in the rigor of the system activities. For example, rationales should be available to explain how high risks were identified. These rationales can then be used to justify the level of documentation between different aspects of functionality and the corresponding amount of evidence collected for testing and qualification. It is worth remembering that a regulator will view the computerized system with a fresh pair of eyes, and obvious viewpoints and decisions may not be self-evident several years after the matter when someone not involved in the initial activity looks at it.

During an inspection, a regulated company may need to provide evidence of the assessment and qualification of their supplier [19]. Where supplier activities and information are leveraged as part of the regulated company's validation for intended use, consideration should be given to the arrangements needed that ensure information on supplier assessment and management processes is available for review.

Holding duplicate copies of supplier information that rightly belongs in the supplier QMS is unnecessary and brings the risk of inconsistency and complexity. The regulated company may consider contractual agreements allowing access to critical supplier documentation under specified extreme circumstances.

For clinical trial specific systems, the EMA Q&A: Good clinical practice (GCP) [20] states that the sponsor or Clinical Research Organization (CRO) must have

“detailed knowledge about the qualification documentation and can navigate in it and explain the activities as if they had performed the activities themselves.”

There must also be established configuration management procedures and documented justification of differences between the supplier’s validation environment and the sponsor’s production environment.

2.3.11 Retirement

Retirement is the last of the system life cycle phases and consists of withdrawal, decommissioning, and disposal. In some situations, a computerized system may be withdrawn from active operations but not immediately decommissioned or disposed of, if it is needed to read retained records/information. This should not be treated as a long-term solution to record readability because systems and software become obsolete over time.

The *ISPE GAMP Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems* [18] details the steps and considerations to complete the retirement, decommissioning, and disposal process.

A key element with planning system retirement is consideration of the data associated with that system. Critical thinking and risk management are needed to effectively evaluate what data needs to be retained, for what period of time, and how, such as:

- Data originally created in this system that has completed its retention period and, as long as there are no legal holds associated with it, may be deleted from the system and/or archived via a formal process.
- Data that is inactive at this stage, i.e., only likely to be needed in an investigation or audit. Based on risk, it may be acceptable to retain this data in a static, easily readable, and portable format.
- Data recently created in the system and may need to stay dynamic for a period of time. Critical thinking is needed here to determine the most efficient way to achieve this and may involve balancing the risk of data migration against the complexity of maintaining a legacy copy of the system.

Data migration may be chosen as a solution to data readability after system retirement to get the existing data into the new system. Data migration is discussed in some detail in *ISPE GAMP 5* [2] and *ISPE GAMP Good Practice Guides* [17]. Automated migration tools provided as standard items by system suppliers are often either assessed in great detail or are used without considering the types of problem data⁵ that might occur within the end-user’s system. The regulated company needs to consider the maturity of the supplier, the robustness of the tool, and how well the tool meets the migration requirement. The assurance of the tool should be focused on actual use cases including any identifiable problem data needed to confirm that it migrates correctly.

Automated test tools may be also leveraged to test the migrated data. Critical thinking is needed for planning how to cleanse and verify that the data is ready for migration, how to assess the quality of the migrated data, how much data needs to be checked, and how any errors created during the migration process may be detected.

⁵ Problem data here is meant data with missing content, data in an incorrect format, data that cannot be handled by the target application, etc.

2.4 Practical Considerations

2.4.1 *Organizational Capability*

People are the source of critical thinking. Critical thinking will only work when used by skilled SMEs with sufficient experience and knowledge.

Organizations need to consider how to build and grow their critical thinking skills within the business. This includes specifically seeking critical thinking skills when recruiting new personnel, incorporating critical thinking into training and development, and ensuring there is a critical thinking element within the balance of team formation.

The mindset and culture of an organization also needs evolve to support critical thinking. Open and constructive discussion between stakeholders is vital to evaluate and challenge the situation, the information, assumptions, and organizational precedents in order to make better decisions based on agreed rationales.

The capability of an organization needs to be proactively grown to become more efficient and effective in its application of critical thinking. The capability build can be measured and consequently steered through a series of levels of increasing maturity, for example:

- Level 1: No application of critical thinking evident in decision-making either by practitioners or by management
- Level 2: Some awareness of critical thinking within the organization but highly variable across individuals and departments
- Level 3: Critical thinking is described in policies and procedures but is inconsistently applied
- Level 4: Critical thinking principles are fully incorporated and routinely applied in working practices
- Level 5: Critical thinking is respected as a core competency with organizational capability continually improved

2.4.2 *People, Process, and Technology*

Guidance around computerized systems tends to focus on technical controls (i.e., software features and functionality) that can be validated as performing as intended. Once validated, the regulated company can be confident that the control will operate to prevent or support the relevant activity, as applicable. However, there is more to a computerized system than software (see Section 2.2.1).

Critical thinking should consider the computerized system within the context of the business processes it supports and the combination of people/process/technology involved. Compliance and fitness for intended use in a process or system requires addressing all components of a computerized system including, but not limited to, its operating environment and interfaces to other systems, the process it supports, and the people operating the process.

The process component of a computerized system can cover (but is not limited to):

- Statistical analysis of clinical trial data
- Process Analytical Technology (PAT) and other manufacturing monitoring and control processes
- Complex analytical laboratory assays
- ERP applications
- Simple workflow with procedural controls

Some of these require validation in their own right – analytical method validation, process validation, etc. – to adequately safeguard patient safety and product quality.

There is also always a level of human interaction present in a process: the people impact. This could be as minimal as simply initiating the process or could include the option for manual intervention or override in the process, which substantially increases risk. Critical thinking should evaluate the level of possible human intervention and its potential impact on the integrity of the data. People controls (procedural and behavioral) are discussed in Section 2.4.3.

2.4.3 Data Governance and Controls

The application of critical thinking skills help ensure data governance and supporting processes are both effective and proportionate. A holistic approach should be taken that includes the technical, procedural, and behavioral controls needed to achieve and maintain data integrity.

Technical controls for data creation, audit trails, access control, data transfers, and storage and archiving are key to effective data management, and are detailed in *ISPE GAMP® Guide: Records and Data Integrity* [7]. Critical thinking for technical controls should consider the controls in other systems or services that support data integrity throughout the data life cycle. With increasing use of external service providers, ownership, retrieval, retention, and security of data needs to be understood. Quality agreements established with third parties need to define the objectives that must be met without being prescriptive as to the methods. An ongoing relationship needs to be established, applying critical thinking and information feedback between the parties so that the objectives are met overall across the business process. Procedural controls should exist as part of the QMS that include policies, procedures, and supporting templates and guidance. Personnel should have the training, facilities, and time to fulfill their roles.

Data integrity is highly dependent upon personal behaviors. Critical thinking plays a key role in establishing effective behavioral controls, recognizing that strength of quality culture varies across different locations driven in large part by geographic values and local historical context. A single approach to quality management and data governance may not be effective in all situations, for example, if cultural differences and dynamics challenge the acceptability of openly reporting problems and challenging hierarchy. Codes of conduct should specifically state behavioral expectations to ensure the reliability and completeness of data, explaining the benefits this brings to patients and the personal consequences for employees who breach controls.

The holistic perspective prompted by critical thinking should ensure the work environment uses technical controls to facilitate simple and effective ways of working. Critical thinking also helps ensure supervisory measures are proportionate to risk, such as, where is it appropriate to have a contemporaneous second person verification versus a later check of completed data activity. Special consideration is needed for hybrid situations where records are compiled from manual and automatic processes to ensure controls are complete and complementary without being overly bureaucratic.

Critical thinking can be used to help identify and target appropriate levels of training for different audiences. Training should cover:

- Human factors for design and use of computerized systems
- Reporting data integrity issues
- Transparent investigation of incidents and issues to understand true root causes beyond the initial reasons so that robust computerized systems are created and maintained

The content of training also needs to be scaled to the detail and reinforcement of principles needed. Training is not necessarily effective if it just repeats earlier content already delivered to the same audience. Trainers should consider fresh and innovative approaches to make training interesting and informative so that its effectiveness is maintained and enhances organizational capability.