GAMP 5 – Validated IT Systems

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.

Quality Risk Management

Chapter 3 introduced the concept of QRM as part of the life cycle approach. This section gives an overview of the

QRM process and Appendix M3 provides more detail.

This section is primarily aimed at new computerized systems. It does not imply that formal risk assessments are

required for all existing systems. The extent of risk management required for existing systems, including the need for

formal risk assessments, should be considered as part of periodic review.

This section focuses on software products and custom applications rather than on infrastructure.

5.1 Overview

QRM is a systematic process for the assessment, control, communication, and review of risks. It is an iterative

process used throughout the computerized system life cycle from concept to retirement.

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

Figure 5.1: Overview and Benefits of Risk Management

For a given organization, a framework for making risk-management decisions should be defined to ensure

consistency of application across systems and business functions. Terminology should be agreed upon, particularly

regarding definitions and metrics for key risk factors.

Such a framework is most effectively implemented when it is incorporated into the overall QMS and is fully integrated

with the system life cycle.

Science-Based Quality Risk Management

Determining the risks posed by a computerized system requires a common and shared understanding of:

• Impact of the computerized system on patient safety, product quality, and data integrity

• Supported business processes

• CQAs for systems that monitor or control CPPs

• User requirements

• Regulatory requirements

• Project approach (contracts, methods, timelines)

• System components and architecture

• System functions

• Supplier capability

The organization also should consider other applicable risks, such as Health, Safety, and Environment (HSE).

Managing the risks may be achieved by:

• Elimination by design

• Reduction to an acceptable level

• Verification to demonstrate that risks are managed to an acceptable level

It is desirable to eliminate risk, if possible, by modifying processes or system design. Design reviews can play a key

role in eliminating risk by design.

Risks that cannot be eliminated by design should be reduced to an acceptable level by controls or manual

procedures. Risk reduction includes applying controls to lower the severity, decrease probability, or increase

detectability.

A systematic approach should be defined to verify that the risk associated with a system has been managed to an

acceptable level. The overall extent of verification and the level of detail of documentation should be based on the risk

to patient safety, product quality, and data integrity, and take into account the complexity and novelty of the system.

The information needed to perform risk assessments may become available, and should be considered, at different

stages in the life cycle. For example, the high-level risks associated with a business process need to be understood

before the risks associated with specific functions of computerized systems can be assessed.3

The criticality of a business process is independent of whether it is manually processed, semi-automated, or fully

automated. Systems that support critical processes include those that:

• Generate, manipulate, or control data supporting regulatory safety and efficacy submissions

• Control critical parameters and data in pre-clinical, clinical, development, and manufacturing

• Control or provide data or information for product release

• Control data or information required in case of product recall

• Control adverse event or complaint recording or reporting

• Support pharmacovigilance

Quality Risk Management Process

The ICH Q9 [14] describes a systematic approach to QRM intended for general application within the pharmaceutical

industry. It defines the following two primary principles of QRM:

• “The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the

protection of the patient; and

• The level of effort, formality and documentation of the quality risk-management process should be

commensurate with the level of risk.”

In the context of computerized systems, scientific knowledge is based upon the system specifications and the

business process being supported.

This Guide uses the following key terms from ICH Q9 [14]:

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

“Hazard: The potential source of harm.”

“Risk: The combination of the probability of occurrence of harm and the severity of that harm.”

“Severity: A measure of the possible consequences of a hazard.”

This Guide applies the general principles of ICH Q9 [14] to describe a five-step process for risk management as an

integral part of achieving and maintaining system compliance. For simple or low-risk systems, some of these steps

may be combined. See Appendix M3 for further details on the QRM process.

This process is focused on managing risks during the project phase. Risk management should also be used

appropriately both within specific activities and during the operational phase. Examples include:

1. Determining the need for supplier audit as part of supplier assessment

2. Determining the rigor and extent of testing

3. Determining corrective actions arising from test failures

4. Determining the impact of proposed changes as part of change management

5. Determining the frequency of periodic reviews

Application of risk management to the above activities is covered in the appropriate sections of this Guide.

Organizations may have established risk-management processes, including the use of methods such as those listed

in Appendix M3. While this Guide describes one suggested approach, it does not intend or imply that these existing

methods should be discarded, rather that they continue to be used, as appropriate, within the context of an overall

QRM framework consistent with ICH Q9 [14].

Process Risk Assessment

Some records and data may reside on more than one system during their life cycle, and QRM activities should start

at the business process level, at a level higher than individual systems. A process risk assessment (also known as

business process risk assessment) is a non-system-specific high-level assessment of the business process or data

flow, which may occur before system-specific QRM activities. An equivalent risk assessment from a data flow (rather

than business process flow) perspective may be performed, using the same approaches and techniques, and with the

same benefits.

The process risk assessment is aimed at identifying key high-level risks to patient safety, product quality, and data

integrity, and identifying the required controls to manage those risks. Typically, at this stage no assumptions are made

about the nature or exact functionality and design of the computerized system(s) that will support the process.

The process risk assessment provides valuable input to subsequent QRM activities. Typical inputs to the process risk

assessment include:

• Defined business process scope

• Process descriptions and/or diagrams

• Identified regulatory requirements for the proposed process scope

• Identified company quality requirements

Step 1 – Perform Initial Risk Assessment and Determine System Impact

An initial risk assessment should be performed based on an understanding of business processes and business

risk assessments, user requirements, regulatory requirements, and known functional areas. A system cannot have a

higher impact than the business process it supports. Any relevant previous assessments may provide useful input,

and these should not be repeated unnecessarily.

The results of this initial risk assessment should include a decision on whether the system is GxP regulated (i.e., GxP

assessment). It also should include an overall assessment of system impact. The scope and objectives of any further

risk assessments should be defined.

Based on this initial risk assessment and resulting system impact, it may not be necessary to perform the subsequent

steps of the process, as the level of risk may already be at an acceptable level.

The specific level of effort, formality, and documentation of any subsequent steps should be determined based on

level of risk and system impact. See Appendix M3 for further details.

If relevant, regulated electronic records and signatures should be identified. Again, existing assessments may provide

useful input and should not be repeated. A detailed approach and specific guidance is provided in the ISPE GAMP

Guide: Records and Data Integrity [35]

Step 2 – Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity

Functions that have an impact on patient safety, product quality, and data integrity should be identified by building

on information gathered during Step 1, referring to relevant specifications, and considering project approach, system

architecture, and categorization of system components. Individual functions cannot have a higher impact that the

system as a whole.

Step 3 – Perform Functional Risk Assessments and Identify Controls

Functions identified during Step 2 should be assessed by considering possible hazards, and how the potential harm

arising from these hazards may be controlled.

It may be necessary to perform a more detailed assessment that analyzes further the severity of harm, likelihood of

occurrence, and probability of detection. See Appendix M3 – Section 11.5 for an example detailed assessment process.

The judgment as to whether to perform a detailed assessment for specific functions should be dealt with on a case-

by-case basis and the criteria can vary widely. The criteria to be considered include:

• Criticality of the supported process

• Specific impact of the function within the process

• Nature of the system (e.g., complexity and novelty)

Appropriate controls should be identified based on the assessment. A range of options is available to provide the

required control depending on the identified risk. These include, but are not limited to:

• Modification of process design

• Modification of system design

• Application of external procedures

• Increasing the detail or formality of specifications

• Increasing the number and level of detail of design reviews

• Increasing the extent or rigor of verification activities

Where possible, elimination of risk by design is the preferred approach.

Step 4 – Implement and Verify Appropriate Controls

The control measures identified in Step 3 should be implemented and verified 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.

The effort, formality, and documentation of the verification activity should be commensurate with the level of risk.

Step 5 – Review Risks and Monitor Controls

During periodic review of systems, or at other defined points, an organization should review the risks. The review

should verify that controls are still effective, with corrective action taken under change management if deficiencies are

found. The organization also should consider whether:

• Previously unrecognized hazards are present

• Previously identified hazards are no longer applicable

• The estimated risk associated with a hazard is no longer acceptable

• The original assessment is otherwise invalidated (e.g., following changes to applicable regulations or change of

system use)

Where necessary, the results of the evaluation should be fed back into the risk-management process. If there is a

potential that the residual risk or its acceptability has changed, the impact on previously implemented risk control

measures should be considered, and the results of the evaluation documented. It should be noted that some changes

may justify relaxation of existing controls.

The frequency and extent of any periodic review should be based on the level of risk and should consider previous

findings and operational history.