International Journal of PharmTech Research
CODEN (USA): IJPRIF ISSN : 0974-4304
Vol.6, No.3, pp 915-919. July-Aug 2014

Quality Risk Management for Computerised Systems- A Review

Sumanth T.N.*, M.N. Raviteja, N. Vishal Gupta, H.V. Raghunandan

Pharmaceutical Quality Assurance Group, Department of Pharmaceutics, JSS College of Pharmacy, JSS University, Sri Shivarathreeswaranagara, Mysore 570015, Karnataka, India.

***Corres.author: sumanthpharmaqa@gmail.com**

Abstract: The review article discusses aboutapplication of risk management principles and tools labeledin Good Automated Manufacturing Practices (GAMP 5), i.e.,Development of Computer Systems in GxP Environment. This article helps to understand impact of computerized systems on safety of the patient, quality of the product and integrity of the data.GAMP 5 relates how understanding of Critical Quality Attributes (CQA) and Critical Control Parameters (CCP) can be applied to computerized systems in the pharmaceutical industry with the intent of using them to the improvement of approaches for validation and verification.Risk management principles applied in various stages of computer system life cycle, i.e., Concept, Project, Operation and Retirement.Based on the risk assessment, necessary verification and validation needs to be recommended for each stage under various category of computer systems (operatingsystem, Standard software package, configurable software packages, and customs software).A Five step approach is used for the risk management of computerized systems.
Key Words: Good Automated Manufacturing Practices, Computer Systems, Critical Quality Attributes, Critical Control Parameters.

Introduction

Over the last three decades, the manufacturing industry has been increasingly using computer systems to control manufacturing processes for improved performance and product quality. Computer systems, however, by the nature of their complexity are susceptible to development and operational deficiencies which can adversely affect their controllability and effect product safety, quality and efficacy. Common examples of such deficiencies include poor specification capture, design errors, poor testing and poor maintenance practice.[1]

In today's competitive and highly regulated environment in the life sciences industry, companies need to focus skilled resources where the risks are highest, thus minimizing risk to patients while maximizing resource utilizations and efficiencies. To achieve this result, it is very essential to appreciate many critical issues. Companies must have a thorough understanding of their business processes and the critical quality attributes of those processes along with appropriate risk management tools.[2]

Risk management techniques have been in use for thirty years. A considerablechange came into existence in 2003 with the prominence given to the acceptability of risk based approach to quality and compliance. The aim was to improve the effectiveness and efficiency of activities by ensuring that controls were commensurate with the risk posed to patients. It was also hoped that this new emphasis would promote early promotion early adoption of new technological advances. Early examples of specific regulatory guidance mentioning risk management for computer systems include

- FDA final Guidance on Scope and application for 21 CFR part 11 Electronic Records; Electronic Signatures[3]
- PIC/S Good practices for computerized systems in Regulated GxP Environments.[4]

Early attempts at risk management were not particularly sophisticated. Risks were often oversimplified, and their management was based on opinion rather than scientific knowledge. Perhaps most crucially, risk management did not typically take into consideration the ultimate impact risks posed to patients. The need for further regulatory guidance was clear. In response, in 2005 the ICH published the consensus expectations from U.S. FDA, European EMEA, and Japanese regulatory authorities for quality risk management. The general principles and process presented were consistent with medical device practices and directly applicable to computer systems. Q9 was incorporated to into U.S., EU, and Japanese GMPs in 2006.

The impact of taking a risk-Based approach to facilities, equipment, and systems was subsequently explored by American Society for Testing and Materials (ASTM) and resulted in the publication of high level guidance in 2007. ASTM promoted the model that emphasized risk management as occurring throughout the life cycle and not just as a discrete activity.[5]

GAMP 4 provided only some basic guidance on risk management for computer systems. The detailed practical guidance becameavailable when GAMP 5 was introduced. The new GAMP-5 guidelines were released February 2008 at the ISPE Manufacturing Excellence Conference in Tampa, Florida. These guidelines are the latest, up-to-date thinking in the approach to validation of GxP computerized systems. The purpose of the guidelines is to "provide a cost effective framework of good practice to ensure that computerized systems are fit for use and compliant with regulation."

GAMP5 guidance aims to achieve computerized systems that are fit for intended use and meet current regulatory requirements, by building up on existing industry good practice in an efficient and effective manner. It provides guidance in the application of risk management principles to the development of computer systems in GxP environments. It is possible to identify potential areas that may fail, and to identify areas with acceptable risk or low risk that can be allotted a lower priority or effort for mitigation.[6]

GAMP 5 categorization enable a high level of evaluation of risk based on the complications associated with software or hardware in combination with common trends of dependability based on ubiquity.Various categories of computer systems as defined by GAMP 5 is given in table 1.

Table 1: Shows different categories of computer systems defined in GAMP 5[7,8]

Category	System (as defined by GAMP 5)
1.	**Infrastructure software** (OS, Middleware, DB managers)
2.	**No Longer used**- Firmware is no longer functionally distinguishable
3.	**Non configured software**- includes default configurable software
4.	**Configured software**- configured to satisfy business process
5.	**Custom software**

Life Cycle Approach within Quality management System

The complete life cycle of a computer system from conception to system retirement should be subject to management and control. It is well known that procedures must be established to ensure that a consistent approach is taken. A separate QMS should exist for computerized systems, rather a single QMS, which covers all activities of an organization including development and use of computer systems.

A life cycle approach entails defining and performing activities in a systematic way from conception, understanding the requirements, through development, release and operational use to system retirement. Figure 1 shows a general specification, design and verification process described in GAMP guide.[8]

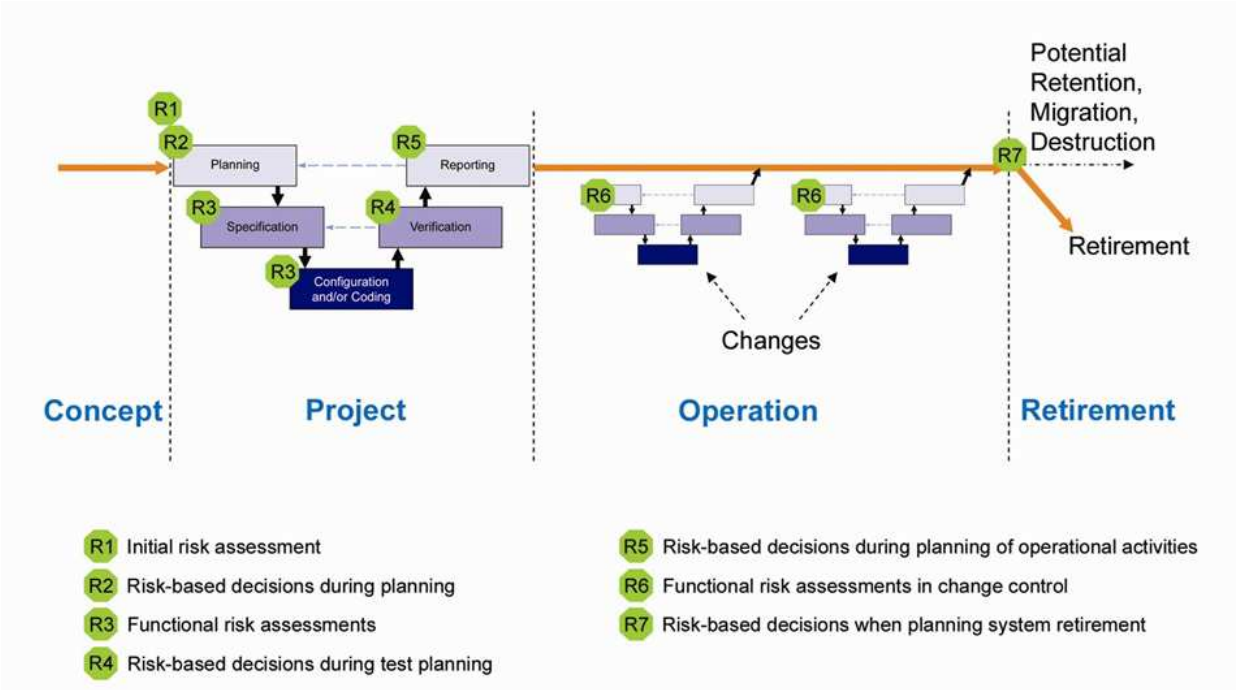

Figure 1.A general specification, design and verification process described in GAMP guide

Quality risk management process

The ICH Q9 describes a systematic approach to quality risk management intended for general application within the pharmaceutical industry. It defines the following two primary principles to quality risk management.

- The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient.
- The level of effort, formality, and documentation of the quality risk management process should be commensurate with the level of risk.[09]

In the context of computerized systems, scientific knowledge is based upon the system specifications and the business process being supported.

GAMP 5 applies the general principles of ICH Q9 to describe a five step process, shown in the figure 2, for risk management as an integral part of achieving and maintaining system compliance.

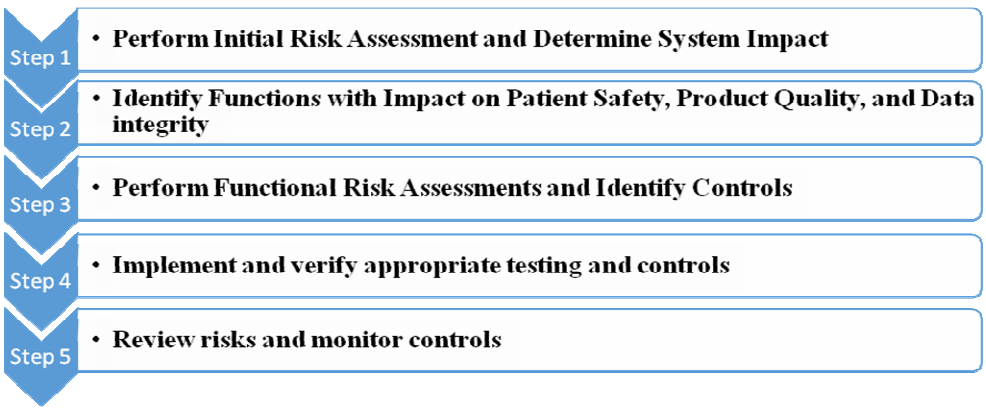

Figure 2: It shows a 5 step process for risk management as given by GAMP 5[8,9]

This process is focused on managing risks during the project phase. Risk management also should be used appropriately both within specific activities and during the operation phase.

Step 1 Initial Assessment

Initial assessment should be done based on an understanding business practices. The understanding can be derived from user requirements, design specifications, operating procedures, regulatory requirements and known functional areas. The assessment should see if whether the system needs to be GxP compliant and include an overall assessment of the system effect. Further it should include an evaluation of the process for impact to patient health, as many of the later steps in this process are reliant on this for the purpose of defining the scale of effort.

Since this step is geared toward understanding the business processes, it is critical to ensure user participation in the assessment and their acceptance of the result.

Step 2 Identify functions with Impact on Patient Safety, Product Quality, and Data integrity

Specific functions that pose risk on safety of the patient, quality of the product and integrity of the data are identified and addressed based on the information got in first step. It must be kept in mind that no function can be evaluated as having greater risk than the process itself. In order, to be able to use the obtained information in third step, functions are enumerated in tabular form. Understanding the system functions' effect on business practices (and finally on patients) is ensured with the user participation.

Step 3 – Perform Functional Risk Assessments and Identify Controls

The functions identified in the step 2 can now be examined by considering likely hazards and what controls may be needed to reduce potential harm. The rigor of the risk analysis can be just adjusted based on the impact of the function as determined in step 2. For low impact systems, no further assessment of failure scenario is necessary. Generic hazards are recognized and evaluated in medium impact systems, for example a generic situation for power loss may be assessed for a data acquisition system.

Specific hazards are analyzed in high impact systems, e.g., electricityproblems that may include simple power failure, power failure with voltage spike, or a voltage drop. For high impact functions, it is helpful to establish a strong link between the ultimate user and the computer system vendor, whose thorough understanding of the system itself can make sure a proper functional risk assessment and right controls identification.

Step 4: Implement and verify appropriate testing and controls:

The appropriate level of challenge testing can be selected, once the severity and risk are thoroughly understood. In general, functions with low risks will need little or no functional testing to meet compliance needs; testing of such functions to meet regular business expectation as defined in the development procedure is ample, for medium impact functions, it is suitable to consider generic failure modes, i.e., consequences of system failure. In the instance mentioned above, this might entail single test case for power loss. The pertinent specific risk scenarios should be tested for high impact systems.

Based in part on the result of testing, controls can be applied. If testing has revealed that the system is good enough, controls may not be necessary or may possibly be emplaced to establish dismissal for high risk functions.

If testing shows some gaps that require remediation, the chosen controls should be appropriate with the evaluated risk. Typically, low risk elements will need only "Good IT practices" this requires the processes and practices that would generally be applied to a well-controlled IT operation for any industry. Medium impact elements will necessitate somewhat more stringent controls, and high impact elements will need even better controls. Controls should be traceable to the recognized risks and want to be verified that they are effective in producing the intended risk lessening. An evaluation of residual should be done for functions primarily determined to be high risk.

Step 5: Review risks and monitor controls

Once the controls are implemented and they need to be reviewed. The employment of the controls may decrease the level of effort for several current activities, such as inspections, assessments, documentation, analysis, and even the degree of quality unit involvement.

After the controls are selected, the remaining risk needs to be assessed to ascertain if the controls are adequate and if the level of risk is acceptable. If the controls are too rigid, a more capablemethod may probably be recommended.

Periodic evaluation after the system is operational will lead to improvement of the practices, controls, and whole risk based approach. The review should

- Consider if previously unrecognized risks are present.
- Determine whetherpreviouslyrecognized hazards are still present .
- Determine if the estimated risk associated with a hazard is no longer acceptable.
- Evaluate if all current controls are still necessary.

The level of risk will determine the frequency of review and when the life cycle the review should occur although review should always be part of the change control practice.[10]

Conclusion

By applying quality risk management principles,risks can be minimized or eliminated in computerized systems used in various functions of pharmaceutical industry. The GAMP 5 QRM strategy offers a realistic approach to computerized system compliance. It appears to be a basis that is adaptable or adjustable and ascendable and assists with the identification and application of controls where they are needed.

References

1. James Agalloco, Frederick J Carleton,Validation of Pharmaceutical Processes. 3rdedition Informa Healthcare Ltd, 2008,607-612.
2. Guy Wingate, Pharmaceutical computer system validation: Quality Assurance, Risk Management and Regulatory compliance.2nd edition,1-10.
3. 21 CFR Part 11 Electronic Records, Electronic Signatures. [Cited 2012 Dec 28]. Available from:http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11
4. Good practices for computerised systems in regulated “GxP” environments http://:www.picscheme.org/pdf/27_pi-011-3-recommendation-oncomputerisedsystems.pdf
5. ASTM E2500-07, “Standard Guide For Specification, Design, And Verification Of Pharmaceutical And Biopharmaceutical Manufacturing Systems And Equipment,” ASTM International, West Conshocken, PA, www.Astm.Org.
6. GAMP 5, A Risk-Based Approach To Compliant GxP Computerized Systems, International Society For Pharmaceutical Engineering (ISPE), Fifth Edition, February 2008, Section-5 Quality Risk Management, www.Ispe.Org.
7. GAMP®5: A Risk-Based Approach to Compliant GxP Computerized Systems. © Copyright ISPE2008. All right reserved. [Cited 2012 Dec 26]. Available from: www.ispe.org/publications/ gam p4togamp5.pdf.
8. ISPE GAMP-5 A Risk-Based Approach to Compliant GxP Computerized Systems, International society for pharmaceutical engineering (ISPE), Fifth edition, Febrauary-2008,– applying management based on the business process. [Cited 2012 Dec 26]. Available from: www.techstreet.com/products /preview/ 1559506
9. ICH HarmonisedTripartate Guideline, “Quality Risk Management Q9,” 9 November 2005.
10. Kevin C. Martin, Dr. Arthur Perez, GAMP 5 Quality Risk Management Approach,The Official Magazine of ISPE vol. 28 No.23, May/June 2008.

*****