Reprinted from
PHARMACEUTICAL ENGINEERING®
The Official Magazine of ISPE
May/June 2008, Vol. 28 No. 3

GAMP 5 Quality Risk Management Approach

by Kevin C. Martin and Dr. Arthur (Randy) Perez

This article describes how the GAMP 5 quality risk management strategy offers a pragmatic approach to computer systems compliance.

Introduction

Background

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 utilization and efficiencies. To achieve this result, it is imperative to understand several critical issues. Companies must have a thorough understanding of their business processes and the Critical Quality Attributes (CQAs) of those processes. This knowledge along with appropriate risk management methods make it possible to identify potential areas that may fail, and to identify areas with acceptable risk or low risk that can be assigned a lower priority or effort for mitigation. It should be possible to reduce or eliminate unwarranted work at all risk levels, but especially on low risk areas, freeing critical resources to mitigate higher risks.

GAMP® 5 provides guidance in the application of risk management principles to the development of computer systems in GxP environments. It has become far less common than it was 10 years ago for life sciences firms to develop their own software. This leads to the generally positive consequence that most software is developed by companies whose continued viability is predicated on their delivery of good software. *GAMP 5* recognizes this fact, a point emphasized by the extensive appendix dedicated to supplier evaluation. It is appropriate to become involved in supplier software development and QA processes only if there is reason to doubt the integrity of these processes.

In this context, this article assumes that software and hardware are developed by the suppliers within a sound quality management system. Therefore, *GAMP 5* stresses consideration of risk to patients with the assumption that risks related to other business issues are covered by the supplier and the customer's standard system implementation processes.

The development of the *GAMP 5* risk management approach has its antecedents in the FMEA-based risk assessment tool published in *GAMP 4* in 2001. The approach matured in the 2005 ISPE *GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures* with incorporation of aspects of ISO 14971 *Medical Devices – Application of Risk Management to Medical Devices.* The expansion of these concepts and the five step approach described in *GAMP 5* and this article are fully compatible with the approaches published in ICH Q9 *Quality Risk Management* (2005) and ASTM E2500 *Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment* (2007).

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

- impact of the computerized system on patient safety, product quality, and data integrity
- supported business processes

Table A. GAMP 5 software categories.

Category	GAMP 4	GAMP 5
1	Operating system	**Infrastructure software** (OS, middleware, DB managers, etc.)
2	Firmware	No longer used — Firmware is no longer functionally distinguishable
3	Standard software	**Non-configured software** — Includes default configurable SW
4	Configurable software packages	**Configured software** — configured to satisfy business process
5	Custom software	Custom Software

- Critical Quality Attributes (CQA) for systems that monitor or control Critical Process Parameters (CPP)
- user requirements
- regulatory requirements
- project approach (contracts, methods, timelines)
- system components and architecture
- system functions
- supplier capability
- the company's risk tolerance

The order in which the above is applied is not as important as ensuring that each area is addressed. However, it is imperative to understand several critical issues. First, it is essential to have a deep understanding of the relevant business processes and to understand CQAs of the processes.

It should be noted that the concept of CQAs is not new. They have been a part of Six Sigma, Mechanical Engineering and Software Engineering quality practices for years. CPPs are also a part of Six Sigma. Thus, these concepts are applicable in a far wider arena than in life science manufacturing; they are an aid to understanding the risks associated with any business process.

GAMP 5 relates how understanding of CQAs and CPPs can be applied to computerized systems in the life science industry with the intent of using them to the development of strategies for validation and verification. With such understanding, it is possible to identify potential areas of the automation that may fail to perform to expectation, and to identify those risk points that can be categorized as low or otherwise acceptable risk versus those that constitute unacceptable risk. It should be possible to reduce, or even eliminate, unwarranted work on low risk issues, freeing resources to be applied to more significant risks.

Although CQAs and CPPs are often identified and employed in relation to manufacturing systems, particularly process control or other computerized manufacturing processes, they are not frequently applied to non-manufacturing areas. However, there is no reason why the concepts should not be applied in other arenas; they can work just as well for a preclinical study as they do for a production line. The approach described in *GAMP 5* describes a framework that can be used in GMP and non-GMP areas equally effectively.

Analysis of CQAs can aid in the development of failure or defect scenarios in order to understand the downstream impact on the patient. With the scenarios identified, the ability to mitigate the risk or impact of the failure can be evaluated, presenting the potential to detect and intercept these faults before serious harm occurs. The ongoing monitoring of not only the process, but the effectiveness of mitigation for potential failure points, can help to reduce the likelihood that the potential failure may become a reality, and if it does, to recognize it early and contain or minimize its impact.

Historic Use of Risk-Based Approaches

Many companies have been using a "quasi-risk based" approach for years. The typical dilemma with validation of computerized systems has been deciding what to test, how much to test, and where should resources be applied to achieve optimum efficiency. Their validation processes often included risk assessments, but without a clear process for using the results of these assessments, they tended to be just another document in one of many binders of validation documentation. In lieu of a sound risk-based approach, these companies tended to err on the side of caution and conduct exhaustive and costly validation exercises.

Requirement documents have been used to help identify key process components, often times weighting them to assign to them a priority based on their relative importance. These types of tools have been used to determine where to focus resources and to identify the critical elements of our processes. Structured approaches such as root cause analysis and Kepner-Tragoe Analysis have been useful in the decision-making process. The critical areas would be documented and tested more than areas of lower criticality. Although the term risk was not necessarily used, the concern was about these critical processes operating properly and not failing. The problem resided in the fact that many viewed compliance as a black and white issue; zero risk meant compliance, and anything less was considered unacceptable.

More recently when 21 CFR Part 11 (August 1997) was first introduced, many formal company assessments included a 'risk filter' where the importance of the electronic record (or signature) was assigned a criticality factor. This was necessary as a part of "triage," deciding what systems needed remediation first. The higher the criticality, the more emphasis would be placed on ensuring that the integrity of the record was maintained. This was done not only for business reasons, but to assure product quality and subsequently patient safety.

Evolution of the Definition and Understanding of Risk

Risk management techniques have been in use for decades, early versions having their genesis in the 1940s. In the 1950s, military and aerospace industries began to apply risk approaches in the form of numerous MIL-STDs. The 1960s saw the creation of reliability engineering approaches (e.g., FMECA and HACCP). Certainly, the surge in the software development and technology industries drove the development of standards, in part impelled by the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996. NIST 800-30 Risk Management Guide for Information Technology Systems is one example. ISO-13485 also was accepted as a risk management standard throughout the product life cycle. The ANSI/AAMI/ISO 14971:2000 was published and applied to risk management of medical devices and replaced both ISO 13485 and EN 1441 (European standard) as the risk standard to be used for compliance in the medical device directives. Other industry standards organizations also contributed (e.g. IEEE, IEC, ISO, SEI, PMI).

The publication of ICH Q9 "Quality Risk Management" in 2005 is having a significant impact on our industry. The FDA, as well as other regulatory bodies, is embracing the Q9

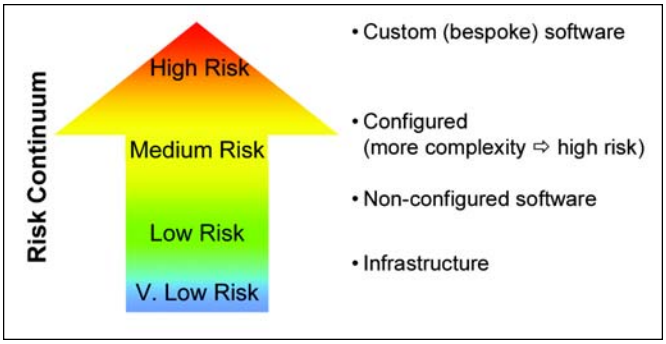

Figure 1. Risk continuum.

concepts. In general, Q9 provides high level guidance regarding:

- hazard identification
- estimating and evaluating risks
- controlling risks
- monitoring the effectiveness of the controls
- documenting the process used for risk management

The Q9 Introduction defines *risk* as the combination of the *probability* of occurrence of *harm* and the *severity* of that harm. It acknowledges the difficulty of achieving consensus or agreement on a risk management approach because of the diversity of the stakeholders. Therefore, with respect "to pharmaceuticals, although there are a variety of stakeholders, including patients and medical practitioners as well as government and industry, the protection of the patient by managing the risk to quality should be considered of prime importance."[1]

The GAMP Categories

The two primary principles of quality risk management are:

- The evaluation of the risk to quality should be based on scientific knowledge and ultimately be linked 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 associated with the process.

One aspect of risk that can be leveraged with respect to computerized systems is the general trend that increased complexity of software implies higher risk for failure due to factors like buggy code, incorrect configuration, or improper implementation. Another unique factor for software is based on ubiquity; for some types of software (e.g., operating systems and database managers), there are so many copies on the market that it is a near-certainty that new faults will not compromise the applications running on them.

The GAMP categories enable a high level evaluation of risk based on the complexity of software or hardware in combination with general trends of reliability based on ubiquity.

When initially introduced, there were five GAMP categories - *Table A*. Since that time technologies have advanced and necessitated a change, which is being introduced in *GAMP 5*.

- The previous Category 1 (Operating Systems) is expanded to include Infrastructure Software and now also includes such layered software components as database managers, middleware, and ladder logic interpreters. Also included are tools used to manage the infrastructure, such as network performance monitors, batch scheduling tools, etc. This class is considered to be low risk due to two primary factors. First, infrastructure software is so ubiquitous that it is extremely unlikely that any unknown faults will exist. Second, this software is challenged indirectly in all other testing activities. While proper function of IT infrastructure may well be critical to satisfying a CQA, infrastructure will almost always have an extremely low probability of failure. Applications built on top of this software may fail, but it will seldom be attributable to failure of infrastructure software.

- Category 2 (Firmware) is no longer a separate category since modern firmware can be so sophisticated that there is no longer any justification for differentiation. Firmware can fit into any of the categories depending on the nature of the embedded software.

- Category 3 (Standard Software) has been renamed Non-Configured Software and includes many examples of firmware. Non-Configured in this sense refers to configuration to meet the needs of a business process; run-time parameters can still be configured. Off-the-shelf software has grown in sophistication to the point where some examples are configurable to meet the business process, and hence

Figure 2. Five step risk management approach. (Source: *GAMP® 5, A Risk-Based Approach to Compliant GxP Computerized Systems*,[8] used with permission from ISPE)

could be considered Category 4. A simplified approach (Category 3) is allowed; however, a user can choose not to configure a simple configurable product and applies the default configuration.

- Categories 4 (Configured Software) and 5 (Custom or Bespoke Software) remain essentially unchanged with the exception that supplier assessments are suggested (i.e., discretionary), depending on the overall criticality of the system, as opposed to requiring supplier audits for all systems within the category.

The GAMP 5 software categories represent a broad indicator of likelihood of software failure. They can be a factor in planning test rigor – but not the only one. Large systems often comprise components of several categories; therefore, each category can help assess overall risk/impact of the components. The complexity of the components also can be useful in evaluating rigor needed for supplier assessment. Risk is a continuum and because the GAMP 5 categories are generalizations, they are not absolute, but can be useful as a tool used in the overall risk process - *Figure 1*. Other significant factors related to the risk of software includes the quality processes of the supplier (it is certainly possible to make bad infrastructure software), the integrity of the implementation process, and of course the use to which the software is put.

The key to maximizing the usefulness of the GAMP categories is to fully realize that they represent general conclusions about wide classes of software, and that they should only be one of the factors considered when planning a validation/verification strategy for a system.

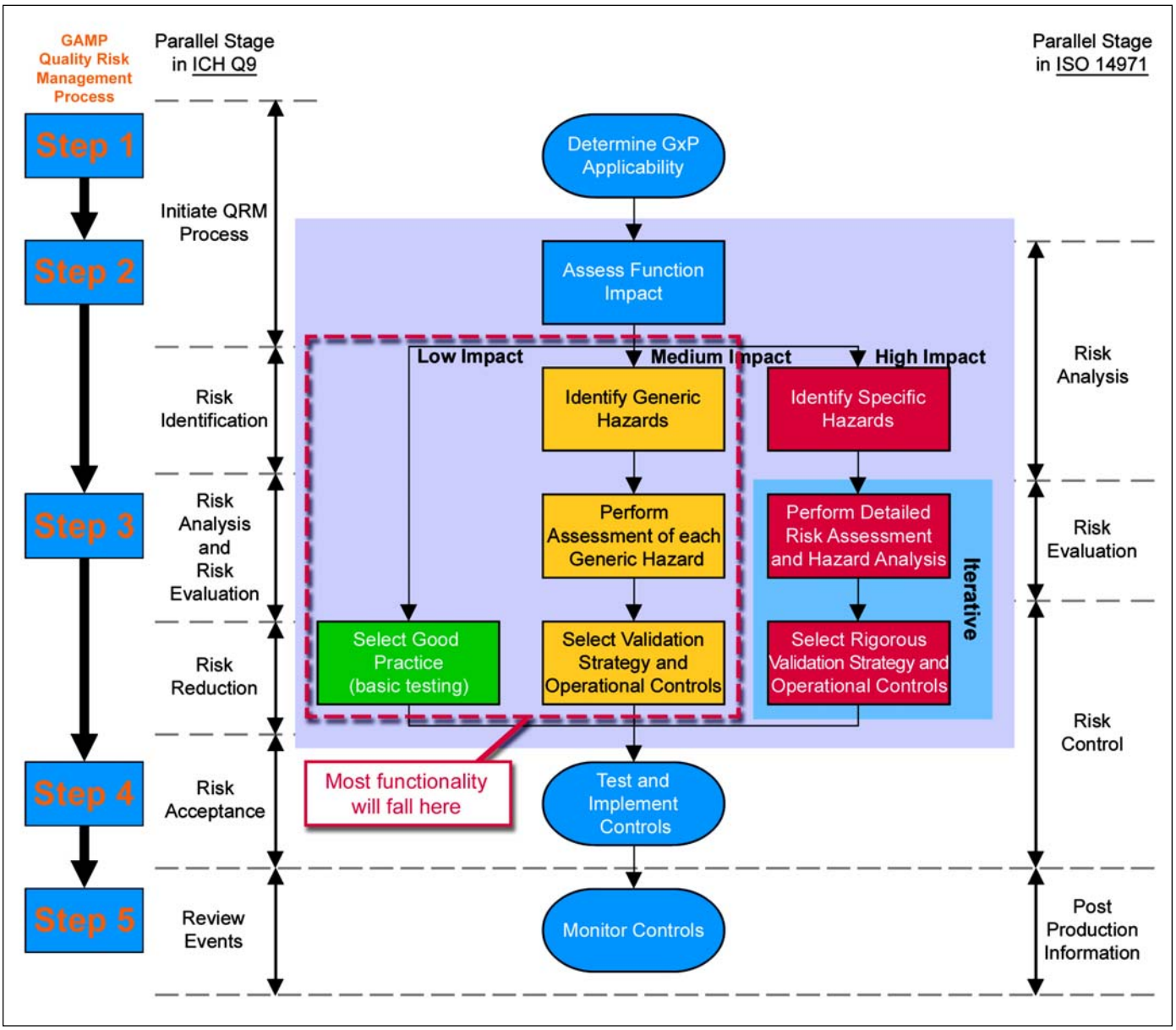

Figure 3. Risk assessment effort scaled according to function impact. (Source: *GAMP® 5, A Risk-Based Approach to Compliant GxP Computerized Systems*,[8] used with permission from ISPE)

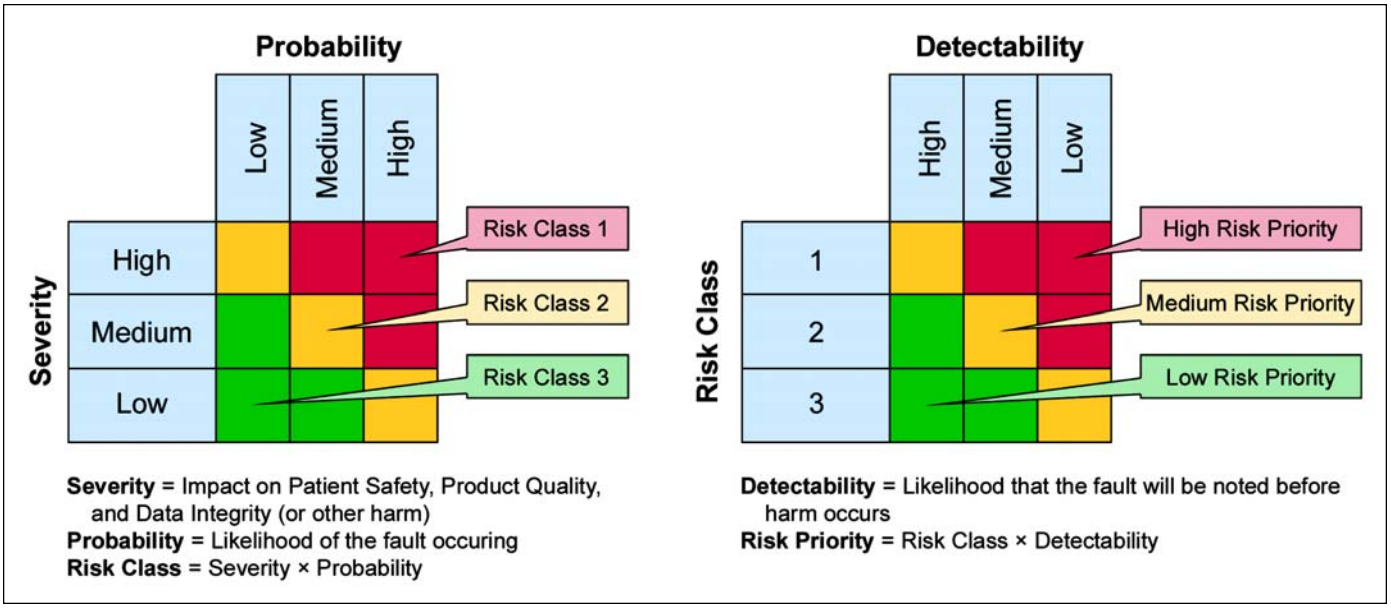

Figure 4. GAMP 5 risk assessment method. (Source: *GAMP® 5, A Risk-Based Approach to Compliant GxP Computerized Systems*,[8] used with permission from ISPE)

Five Step Approach to Risk Management for Computerized Systems

Guiding Principles

GAMP 5 is a science-based approach to understanding and managing risk for computerized systems. It is focused on a 'top-down' approach that looks at *processes* before *systems* or *functions*. Determining the impact to patient health for automated systems is not possible without a thorough understanding of the underlying business processes. Further, the risk associated with a computerized system cannot be greater than the risk associated with the processes it supports. The approach is forward looking in that it is compatible with new initiatives, such as the forthcoming ISPE Baseline® Guide that will present an alternative approach, and aligns well with the recently published ASTM 2500-07 standard. Although there are many existing standards available, ISO 14971 and particularly ICH Q9 were selected as the foundation for the *GAMP 5* Quality Risk Management (QRM) approach.

The central tenet of the *GAMP 5* approach is to define acceptable practices and apply stronger measures only where warranted. The approach should be simple in that an assessment result should indicate where additional controls are needed based on the relative risk. An added benefit by keeping the approach simple is that there should be only minimal impact when a company transitions from old compliance programs to new ones.

Process Description

It should be noted that organizations may have already established processes for risk management. While GAMP 5 provides one suggested approach, it does not intend that companies discard their current practices, rather that they continue to be used as appropriate within the overall quality risk management framework consistent with ICH Q9.

The *GAMP 5* Quality Risk Management approach is based on a simple five step process - *Figure 2*, where the emphasis is on constantly narrowing the focus to the point where rigorous testing and additional controls are only applied where the risk warrants.

Step 1 – Initial Assessment

An initial assessment should be performed based on an understanding of the business processes. The understanding can be derived from user requirements, design specifications, operating procedures, regulatory requirements, and known functional areas. The assessment should include a decision on whether the system is GxP regulated and include an overall assessment of the system impact. Further, it should include an evaluation of the process for impact to patient health, as many of the later steps in this process are dependent on this for the purpose of determining the scale of effort.

Since this step is geared toward understanding the business process, it is critical to ensure user involvement in the assessment and their acceptance of the outcome.

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

Building upon the information obtained in Step 1, the specific functions that have impact on patient safety, product quality, and data integrity can be identified and addressed. It must be remembered that no function can be assessed as having higher risk or impact than the process itself. The functions are typically listed in tabular form to be used in Step 3. Similarly to Step 1, user involvement is important to ensure that the impact of a system function on the business process (and ultimately on patients) is understood.

Step 3 – Perform Functional Risk Assessments

and Identify Controls

The functions identified in the previous step can now be analyzed by considering possible hazards and what controls may be needed to minimize potential harm. A company's risk tolerance is also a factor to be considered when selecting possible controls. The rigor of the risk analysis can be adjusted based on the impact of the function as determined in Step 2 - *Figure 3*. For low impact functions, no further assessment of failure scenarios is warranted. For medium impact systems, generic hazards are identified and assessed, for example, a generic scenario for power loss might be assessed for a data acquisition system. For high impact functions in this system, specific hazards are analyzed, e.g., power problems that might include simple power failure, power failure with a voltage spike (lightning), or a voltage drop (brownout). For high impact functions, it is helpful (and recommended) to establish a strong link between the final user and the computer system supplier, whose deep knowledge of the system itself can ensure a correct functional risk assessment and suitable controls identification.

To execute these assessments, *GAMP 5* retains the simple FMEA-derived risk assessment process described in *GAMP 4 - Figure 4*. After identifying potential hazards, severity is plotted against the probability of occurrence to obtain the Risk Class. The Risk Class is then plotted against detectability to obtain the Risk Priority. Conveniently, this assessment lends readily itself to a semi-automated documentation approach using a spreadsheet.

As Figure 3 also illustrates, this process is aligned with the defined process steps of ICH Q9 and ISO 14971.

Step 4 – Implement and Verify Appropriate Testing and Controls

Once the severity and risk are understood, the appropriate level of challenge testing can be selected. Figure 5 illustrates the concept of planning testing and selecting controls based on assessed risk and impact. In general, functions with low risk will require little or no functional testing to meet compliance needs; testing of such functions to meet normal business expectation as defined in the development methodology is adequate. For medium impact functions, it is appropriate to consider generic failure modes, i.e., what will happen if the function fails. In the example mentioned above, this might entail a single test case for power loss. For high impact systems, the relevant specific risk scenarios should be tested. In the example above of power problems, test cases might be executed for each of the three cases noted (power loss, power loss accompanied by a voltage spike, and brownout conditions).

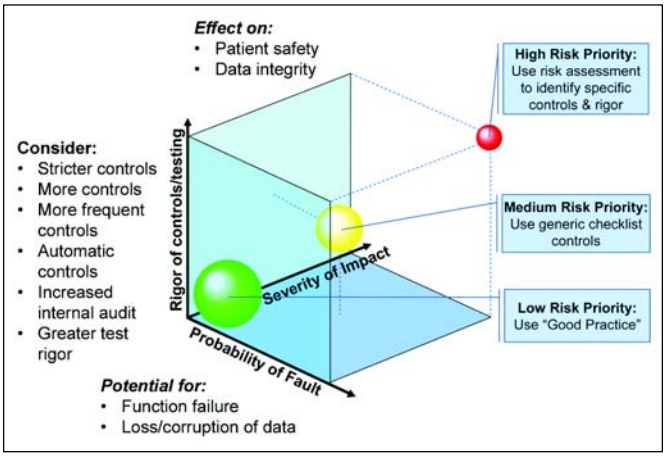

Figure 5. Relationship of risk, severity, and control.

Based in part on the outcome of testing, controls can be applied. If testing has shown that the system is robust enough, controls may not be warranted or may perhaps be emplaced to establish redundancy for high risk functions.

If testing reveals some gaps that need remediation, the selected controls should be commensurate with the assessed risk. Typically, low risk elements will require only "Good IT Practices." This entails the processes and practices that would normally be applied to a well-controlled IT operation for any company. Medium impact elements will require somewhat stricter controls, and high impact elements will require even greater controls. Controls should be traceable to the identified risks and need to be verified that they are effective in producing the intended risk reduction. An assessment of residual risk, i.e., the risk status following the application of the selected controls, should be performed for functions initially determined to be high risk.

Step 5 – Review Risks and Monitor Controls

Once the controls are implemented, they need to be monitored. The implementation of the controls may reduce the level of effort for many current activities, such as audits, assessments, documentation, testing, and even the degree of quality unit involvement. By communicating the resultant impact of implementing these controls, other benefits may be realized such as:

- benchmarking against standards
- measuring the amount of value added to the process
- determining the cost, regulatory, and legal impact
- developing a Risk-Based ROI model

After the controls are selected, the residual risk needs to be evaluated to ascertain if the controls are adequate and if the level of risk is acceptable. If the controls are too stringent, a more efficient approach may possibly be suggested.

Periodic evaluation after the system is operational will lead to improvement of the processes, controls, and overall risk strategy. The review should

- consider whether previously unrecognized risks are present
- determine if previously identified hazards are still present (and to what level)
- ascertain if the estimated risk associated with a hazard is no longer acceptable
- evaluate whether all existing controls are still necessary

The level of risk will determine the frequency of review and when in the life cycle the review should occur although review

should always be part of the change control process. As in any aspect of risk management, the activity should ideally be a team-based exercise.

Summary

The GAMP 5 QRM strategy offers a pragmatic approach to computer systems compliance. It avoids reliance on a single standard that can be excessive and/or inadequate, and is consistent with ICH Q9 and has incorporated some elements from ISO-14971. It is a framework that is flexible and scalable and assists with the identification and application of appropriate controls where they are needed.

References

1. ICH Harmonised Tripartite Guideline, "Quality Risk Management Q9," 9 November 2005, p. 1.
2. *ISPE Baseline® Pharmaceutical Engineering Guide, Volume 5 - Commissioning and Qualification,* International Society for Pharmaceutical Engineering (ISPE), First Edition, March 2001, www.ispe.org.
3. ASTM E2500-07, "Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment," ASTM International, West Conshohocken, PA, www.astm.org.
4. "Global Risk Management: Challenges in Risk Management of Automation Systems," GAMP Forum, August 2005; Steve Coates, Wyeth/GAMP Risk Management SIG Chair.
5. "Using Science-Based Risk Management to Develop Compliant Computer Systems," ISPE Annual Meeting 2007; Randy Perez, PhD, Novartis Pharmaceuticals/GAMP Americas Chair.
6. FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures - Scope and Application (2003).
7. ICH Harmonised Tripartite Guideline, "Quality Risk Management Q9," 9 November 2005.
8. *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.
9. *GAMP® Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures,* International Society for Pharmaceutical Engineering (ISPE), First Edition, April 2005, www.ispe.org.
10. Kepner-Tregoe Analysis, ©2006 Kepner-Tregoe Inc. www.kepner-tregoe.com.
11. ISO 14971, "Application of Risk Management to Medical Devices," December 2000, www.iso.org.

Acknowledgement

We would like to express my gratitude to the members of the GAMP Risk Management SIG and GAMP Steering Committee who reviewed and provided substantive comments, and in particular, Steve Coates whose leadership was a driving force for this article.

About the Authors

Kevin C. Martin is Vice President of Regulatory Compliance Business Development for CimQuest-Vantage LLC, and has more than 30 years of pharmaceutical industry experience that includes management positions at Wyeth and McNeil Pharmaceutical. He is considered a subject matter expert for computer systems compliance within the QA, IT/IM, Manufacturing/Operations, Clinical, and R&D environments. He is a former member of the PhRMA Computer Systems Validation Committee, a former chair of the ISPE DVC CSV Sub-Committee, was a Core Team member for the PDA Part 11 Task Group, is a member of the GAMP Americas Steering Committee and is the GAMP Americas Sponsor to the Risk Management SIG. Martin holds a BS in chemistry from Delaware Valley College of Science and Agriculture and a Master of Engineering in manufacturing systems from Penn State University. He can be contacted by telephone: +1-215-260-6327 or by e-mail: kevin.martin@cimquest.com.

CimQuest-Vantage LLC, 35 E. Uwchlan Ave., Suite 330, Exton, Pennsylvania 19341, USA.

Dr. Arthur (Randy) Perez, Executive Expert, IT Quality Assurance for Novartis Pharmaceuticals, has served on the ISPE International Board of Directors since 2005. His responsibilities at Novartis include a wide range of IT Compliance issues, such as GxP, Sarbanes-Oxley, and data privacy. He serves on several global Novartis teams dealing with computer systems compliance issues, and has authored many of the firm's global GxP compliance policies. During his 25-year tenure at Novartis, he has developed a broad range of experience, working as a chemistry group leader in process research, managing a chemical manufacturing process validation program, and running a QA validation group for pharmaceutical operations. He was a member of the PhRMA Computer Systems Validation Committee and was instrumental in the formation of GAMP Americas when that group started in 2000. He initiated and led the Global Information Systems SIG, which wrote a GAMP® Good Practice Guide that was published in 2005. In 2002, he was elected Chairman of GAMP Americas and became a member of the global GAMP Council. Perez has been a speaker and a course leader at numerous ISPE Continuing Education seminars in the US and Europe, and has been published in industry journals and textbooks. He can be contacted by telephone: +1-862-778-3509 or by e-mail: arthur.perez@novartis.com.

Novartis Pharmaceuticals, One Health Plaza, East Hanover, New Jersey 07936, USA.