FALL 2016 • Volume 15/Issue 3 • ISSN 1538-8786

BioProcessing JOURNAL

Trends & Developments in BioProcess Technology

A Production of BioProcess Technology Network

BioProcessing JOURNAL
TRENDS & DEVELOPMENTS IN BIOPROCESS TECHNOLOGY

The First of a Three-Part Series

Quality Risk Management (QRM):

Identifying, Evaluating, and Mitigating Threat Risks to Biopharmaceutical Enterprises

By Mark F. Witcher

Abstract

The FDA's ICH Q9 quality risk management (QRM) guidance material is the foundation for understanding and evaluating patient risks associated with developing and manufacturing pharmaceuticals.[1] This three-part paper describes approaches a team of subject matter experts (SMEs) can use for implementing two important applications of QRM. Part I provides a method for identifying and remediating threat risks that may affect the product's quality or other important aspects of a manufacturing enterprise's lifecycle, from product research and development to commercial manufacturing. The second QRM application covered in Part II manages patient risks by identifying, evaluating, and managing risks associated with process parameters (PP) on the product's critical quality attributes (CQAs). The final paper, Part III, describes an approach for accepting or further mitigating the risks evaluated by the QRM exercise.

Introduction

The purpose of this first paper is to provide an approach, conceptual understanding, and tools for performing a QRM exercise for identifying, analyzing, and managing a wide variety of risks from threats associated with designing, building, and operating pharmaceutical manufacturing facilities. This paper does not address the methods used by either the subject matter expert (SME) team or management to accept or reject the risks identified and managed by the QRM exercise. It also does not address the formation, selection of members, or subsequent training of the SME team.

In the much-referenced guidance for industry document, ICH Q9 QRM, risk is vaguely defined by the FDA as "*the combination of the probability of occurrence of harm and the severity of that harm.*"[1] The topic of "risk" has a long and illustrious history covering most, if not all of humanity's endeavors.[2, 3] Various kinds of risk have been analyzed and subjected to a wide spectrum of viewpoints and biases based on individual beliefs, appetites, and priorities.[4, 5] To some, risk is the adverse consequence of something occurring that is undesirable and causes harm to someone or something. To others, risk is primarily the uncertainty that an adverse consequence might occur. Also, risk might be considered an uncertain threat or hazard that could result in an adverse consequence. The approach described in this article provides a method to evaluate and manage all of the above-mentioned viewpoints.

Evaluating and managing risks requires a framework and lexicon that provides structure for SME teams to share and exchange concepts and ideas using commonly agreed upon tools and terminology. The structure must also facilitate the effective communication of the risk elements and the essential features of the analysis to all parties involved, including management for decision-making and regulatory agencies for approving the product.

Currently used QRM approaches and tools result in widely varying outcomes and frequently do not accomplish the goals of clearly identifying, analyzing, and managing risks for control and acceptance.[6] Many of the most commonly used tools, such as failure modes and effects analysis (FMEA), failure modes, effects, and criticality analysis (FMECA), and other risk matrix tools are frequently poorly understood and misapplied.[6–11] The purpose of this paper's framework is to provide a sequential methodology and lexicon for effectively applying QRM to a wide range of product development activities and biomanufacturing enterprise systems.

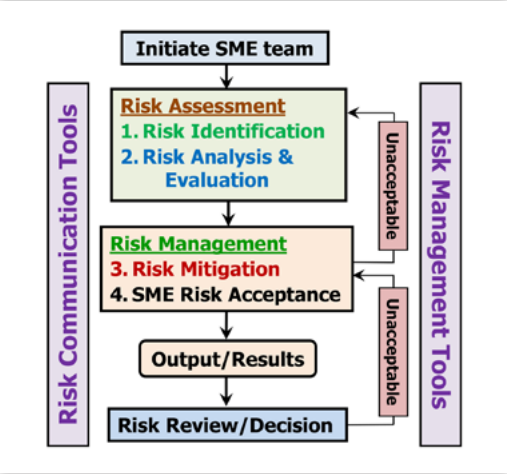


FIGURE 1. A summary of the QRM process, as described in ICH Q9. The paradigm describes the identification, analysis/evaluation, mitigation, and acceptance of risks by a team of SMEs. The recommendation of acceptance depends on the team's assessment of the risk's severity. Acceptance by management is based on effective communication of the risk and its analysis and management by the SME team.[1]

The QRM process described in ICH Q9 is summarized in **Figure 1**. The QRM exercise is performed by a team of SMEs assembled to perform the following four steps:

1. **Risk Identification**—For a process, or process network (system), identify the adverse consequences that can be produced by the system.
2. **Risk Analysis and Evaluation**—For the risks identified, perform a structured analysis of the risk's elements and evaluate the factors that influence the likelihood and severity of the consequence.
3. **Risk Mitigation**—For the risks evaluated, mitigate the likelihood of the risk occurring to an acceptable level by modifying or adding a process.
4. **Risk Acceptance**—After the risks are evaluated and then mitigated (if required), the SME team must effectively communicate and recommend acceptance of the risks and the required investment for mitigation.

This paper focuses on the first three steps and does not deal specifically with the complex give-and-take discussions required for reaching a group consensus on accepting or rejecting risks by either the SME team, or ultimately by management. The acceptance decision is discussed in Part III of this article series.

As shown in **Figure 1**, the QRM exercise is supported by risk management and communication tools for carrying out and communicating the four steps. One of the goals of this paper is to provide the tools needed to facilitate communication of the risks and their analysis to the decision makers. To understand the QRM exercise, we begin by looking at the elements associated with risks to provide understanding and establish a specific sequence of activities for identifying, analyzing, mitigating, and eventually communicating the risks.

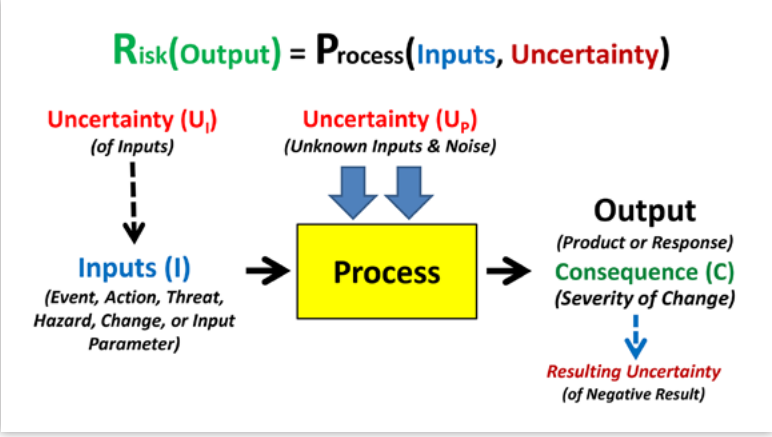
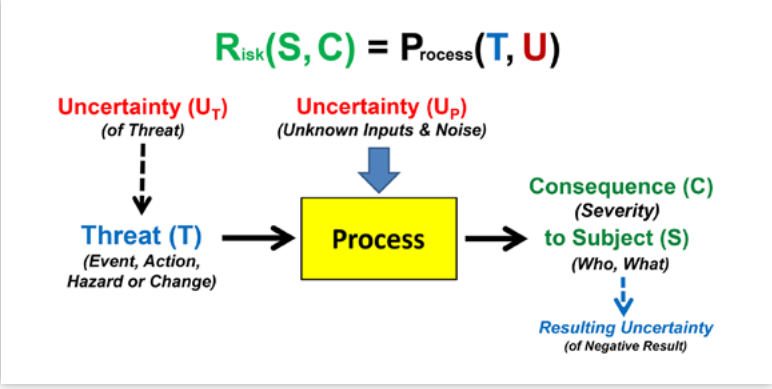


FIGURE 2. A generalized risk structure based on the input-process-output model of Aven.[12] The emphasis of this model is on understanding the uncertainty and control mechanism of the process that passes the inputs to result in the risk's output defined in terms of a negative consequence.



Understanding Process-Based Risk Models

A general risk definition based on an input-process-output model is shown in **Figure 2**.[12] The focus of this approach is the process. Identifying and understanding the processes through which the inputs, or in this case the threats, pass is key to understanding the mechanisms for controlling the consequences of the inputs being evaluated.

Since the topic of this paper is to manage threats, the model in **Figure 2** is adapted to a model shown in **Figure 3** that has threats as the input to the process. The generalized model in

FIGURE 3. The generalized threat-process-consequence model adapted for evaluating threat risks. The threat or hazard in the form of an input event passes through the process to produce a consequence to the subject. The mechanism by which the threat produces the consequence cannot be understood without a clear definition and understanding of the process.

Figure 2 can be adapted a variety of ways to deal with many types of risks. A practical adaptation will be shown in Part II of the article series for appropriately assessing product quality risks from process parameters.

Because threats can have a wide range of consequences, the risk process's output has two elements that must be identified. The first element to identify is the subject of the risk. The second is the consequence to the subject that results from the threat.

Risk is an undesirable output consequence from a risk process described by the following model elements:

Risk Subject (S)—The "who or what" (target, thing, business, person/victim, or group) negatively affected by the consequence. For biopharmaceuticals, the most important risk subject is product quality, which is usually measured by critical quality attributes (CQAs). Most QRM exercises should begin with threats to product quality before dealing with other risk subjects. However, the subject being evaluated can include worker safety, business risks, and a wide variety of operating risks that could negatively affect the enterprise's ability to successfully make product.

Consequence (C)—The negative outcome or the result of the risk that affects the subject. Consequence can be viewed as a bad output from the risk process. Risk consequences are measured in terms of severity to the risk subject. The uncertainty of the consequence is derived from the uncertainties of the threats and the process's performance. When the subject is product quality, the negative consequence is variation in product CQAs or process performance away from the desired state, value, setpoint, or specification. For example, contamination in the product would be one form of negative consequence that could result from a wide variety of internal and external threats.

Threat (T)—The event or hazard that results in the consequence. Threats are viewed as bad or undesirable inputs to the risk process. Depending on how the risk process is defined, the threat may be an external event or input that passes through the process to result in the consequence, or the threat may be generated internally to the process as initially defined. The threat may or may not be measurable or detectable depending on how the risk process is defined.

Risk Process (P)—Any process producing the consequence. In most cases, a threat passes through the process to result in the consequence. The risk process may range from a very simple process (*e.g.*, a piece of equipment or a straightforward practice used to operate a piece of equipment) to very complex systems such as an entire manufacturing facility.

For biopharmaceutical manufacturing, the risk processes (or system) are typically complex combinations of equipment and procedures networked together to control both the quality of the product and the performance of the process. While risk threats and consequences can be identified and initially evaluated without a clear understanding of the risk process, an accurate assessment of uncertainties and threat remediation requires a more complete identification, definition, and understanding of the risk process. Complex systems may have to be described as complex networks of individual processes with their own set of inputs and outputs in order to understand and access the relevant detail required for the QRM exercise.

Uncertainty (U)—The propagation of the threat through the process has a number of uncertainties associated with the possibility of the threat occurring and the process's ability to control, minimize, or eliminate the threat to prevent or reduce the likelihood of the consequence. Because uncertainty is described in this approach in qualitative terms, "likelihood" will be used to describe the various uncertainties of the risk. Because probability is a mathematical term used as a quantitative measure of uncertainty governed by specific mathematical principles, it is not used in this approach.

Figure 3 provides an intuitive model of the threat risk's elements. The effectiveness of the QRM process is determined by the amount of information and understanding of the five elements. However, the definition of the process is especially important. How the process is defined becomes the foundation for the completeness of the analysis. The uncertainty of the consequence is modified as the result of changing the risk process by adding control features to decrease the likelihood and impact of threats on the output of the process and thus, the likelihood of the consequence. New processes can also be added to remediate threats. However, improving existing processes should always be investigated prior to adding new processes. We continue by examining the process and its definition in the form of a model as the basis for the QRM exercise.

Understanding Risk Process Models

Risk analysis and management is performed using some type of model. The models range from an intuitive understanding based on experience to a full-scale experimental implementation of the process. Most models used by SME teams are based on their understanding and experience with similar models or systems. In some cases, small-scale lab or pilot process models tested by design of experiment (DoE) methods are used for further understanding, gathering data, and gaining experience.

Processes can include equipment, people, methods, procedures, or a variety of combinations. As we shall see, processes can range from simple procedures, personnel training programs, and raw material screening tests to complex process equipment with sophisticated sensors and control systems designed to handle a variety of threats in the form of bad inputs or changes in input parameters.

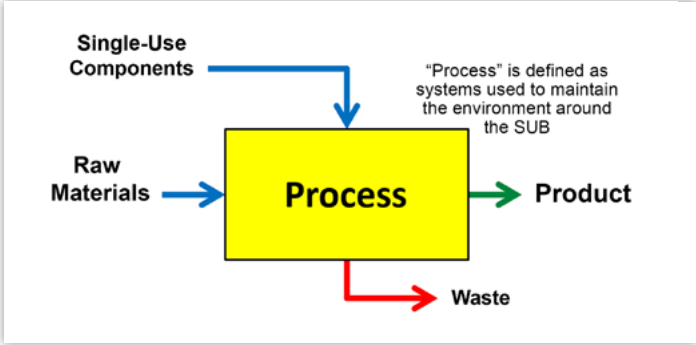


FIGURE 4. A process model for the environment around a single-use bioreactor (SUB) system showing inputs and outputs. The subject of the risk is the SUB's surrounding environment. The consequence is a contaminated environment from the threats involved in setting up, operating, and cleaning the SUB.

A model for the environment around a SUB process is described in **Figure 4**. Primary inputs to the process for this analysis are the single-use components used to operate the SUB and the raw materials, including the media and cells grown in the bioreactor. Outputs are the product manufactured in the SUB and a substantial amount of solid waste after the run is completed.

The risk process can be defined as shown in **Figure 4** for the initial evaluation of the risks in a wide variety of ways. A more detailed analysis of the same process is shown in **Figure 5**. By evaluating the process network in **Figure 5**, the uncertainty of the threat's realization as a contamination of the SUB's environment is defined by looking at all of the subprocesses. Evaluating the network of processes and modifying them to reduce the likelihood of the threat's impact being realized by the key elements of the process network can reduce the likelihood of a contaminated environment surrounding the SUB.

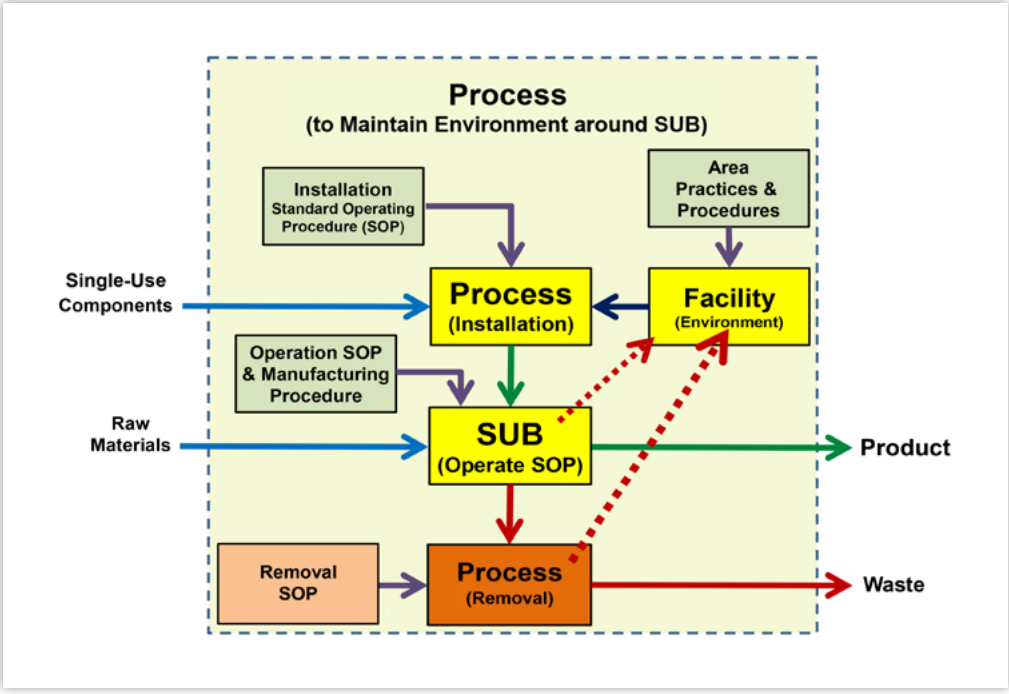


FIGURE 5. Expanded model of Figure 4 that includes a process network containing support processes for setting up, operating, and cleaning the SUB. The systems have four relevant practices and procedural processes that affect the performance of the system. In this case, the risk consequence is contamination of the SUB's surrounding environment. Two of several possible threats, shown with the red dotted arrows, can arise from operating the SUB and removing used single-use components.

The uncertainty (or likelihood) of a threat-initiated risk is modified by improving an existing process or adding a new process to the process network. Process modifications may include new or improved control systems using the principles of process analytical technology (PAT) to detect, dampen, or remove threat inputs such that the consequence output is not realized.[13] In this example, the procedural SOPs and their execution play a major role in the uncertainty of the contamination likelihoods. If needed, improving and then executing SOPs through better training may be the best method to decrease the contamination threats.

Before further developing the QRM methodology, a method for rating risks is required.

Rating Risks (Continuum of Criticality)

The most common method of rating a risk, or comparing multiple risks, is an index composed of the likelihood and the severity of the consequence on the subject. In this framework, a risk index composed of the mathematical product of the risk's consequence likelihood and severity is recommended. Depending on the risk tool, the index can be generated based on the risk element scores determined by the SME team using a four-point scale shown in **Table 1**. Other rating systems are possible, depending on the SME team's preferences.

Risks should not be rated or classified into broad categories such as critical, key, or non-key, but instead, rated relative to each other for further evaluation. The risk matrix score does not always provide an accurate picture of every risk.[6,7] For example, despite the fact that they receive the same risk index value, a very rare but catastrophic consequence (*e.g.*, death) is not the same as a near certain, but insignificant consequence (*e.g.*, discomfort). The risks are totally different and must be treated as such by the SME team when making acceptance decisions. The criteria for accepting or not accepting a risk should not be based purely on the risk index, but rather, on an overall analysis of the entire risk.

Because a wide variety of factors are involved, the QRM exercise has a high degree of intrinsic variability, regardless of the method employed. When used for making decisions, the variability of the results of each QRM exercise must be respected. The exercise's results and variability must be documented in a manner that allows for future analysis when additional information and understanding becomes available.[6] All risks must be individually evaluated and rated based on their relative impact on the risk subject being considered.

The more that is known about all the elements, the more effectively risk can be correctly identified, evaluated, managed (if necessary), and then accepted. A fundamental concept in biopharmaceutical manufacturing is that all risks, including those that are have not been identified or evaluated are *de facto* accepted regardless of their potential severity. In addition, risks that have been incorrectly evaluated or improperly managed are also accepted into the course of product manufacturing.

By combining the QRM methods (**Figure 1**) with a threat risk model (**Figure 3**) and rating system (**Table 1**), a sequential QRM approach can be developed.

TABLE 1. Four-point risk rating matrix. This is computed as the mathematical product of the SME team's ratings of the likelihood and severity of the consequence.

U_I = Initial Uncertainty U_T = Threat Uncertainty U_P = PAT Uncertainty U_F = Final Uncertainty			Severity of Consequence (C)			
			Insignificant ≤0.1× 1	Minor ~× 2	Major (Little Known) ~10× 3	Catastrophic (Unknown) ≥100× 4
Likelihood of Consequence	≥ ~10%	4 Near Certainty (Unknown)	4	8	12	16
	~ 1%	3 Likely (Little Known)	3	6	9	12
	~ 0.1%	2 Possible	2	4	6	8
	≤ ~ 0.01%	1 Rare	1	2	3	4

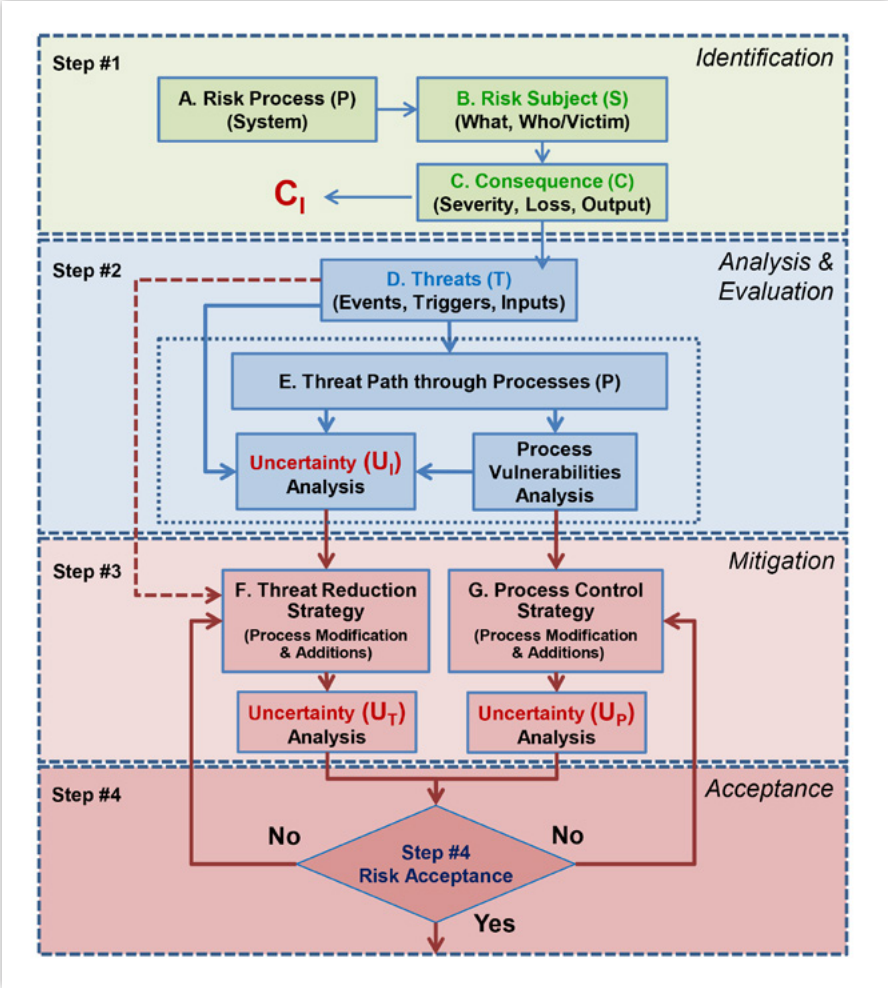


FIGURE 6. QRM threat risk methodology. The four ICH Q9 steps shown in Figure 1 have been expanded to include seven elements: **A–C** identify the risk process, subject, and consequence; **B–E** identify, analyze, and evaluate the threats that may pass through the risk process to result in the consequence; and **F–G** develop control strategies using a more detailed analysis of the process to mitigate the impact of the threats. In the acceptance Step #4, the risk is either accepted or additional process modifications are made to further mitigate the threats.

QRM Approach for Threat Risks

We begin by defining and expanding each step shown earlier in **Figure 1** to a more detailed sequence (**Figure 6**). The risk elements defined in **Figure 6** identify, analyze, evaluate, and mitigate the risks using the QRM process. To aid in risk communication, a spreadsheet containing items A–G from **Figure 6** can be easily assembled and used to guide the QRM discussion through the identification and mitigation sequence. A possible spreadsheet is shown in **Table 2** (on the following page).

Step #1: Identification

The first task is to identify the overall process or system of processes being evaluated. The process shown in **Figure 4** is an example. As stated previously, the process can be a single piece of equipment, a unit operation (UO) such as a bioreactor system, a sequence of UOs, or an entire biopharmaceutical manufacturing facility.

The second task is to identify the risk subject. Mixing risk subjects such as product quality and personnel safety makes the analysis less focused. When dissimilar risk subjects must be considered, the QRM exercise should be subdivided to keep the focus of the discussion on the appropriate risk subject. Patient safety, *per se*, does not make a good risk subject because the patient is far removed from the manufacturing operation. Patients are subjected to a large number of uncertainties unrelated to product manufacturing. However, patient safety is assured by the production of an invariant product based on the specifications defined through process experience and product testing, particularly during clinical-phase testing.[14]

The third task is to identify and rate the negative consequences that the risk subject may experience. The consequences can be described in terms of the severity of

the loss as defined in the beginning of the analysis.

Step #1 (as shown in **Figure 6**) can be summarized by the following three tasks:

A. Initial Risk Process—The SME team agrees on a summary definition of the system or process to be evaluated, such as **Figure 4's** summary process.

B. Risk Subject—A definition of what or who suffers the loss or negative impact. The SME team may want to brainstorm a set of risk subjects to be covered by the exercise. For biopharmaceuticals, the quality of the product is a primary risk subject that should always be addressed. The risk subject example illustrated in **Figure 4** addresses the environment around the SUB.

C. Consequence—A brief statement of risk consequence to the subject, in terms of the loss or negative results. Based on the description, the consequence rating is estimated as a measure of its severity. In this framework, the four-point rating scale for consequence severity shown in **Table 1** is recommended for calculating the consequence index (C). In **Figure 4**, for example, the consequences of a contaminated SUB environment might have significant safety consequences to the operating personnel in the area.

Variation in product quality against release specifications can have a variety of consequence severities. Obviously, final product that does not meet release specifications can have significant consequences. Variability in product attributes, or in the process's performance (to be discussed in Part II) may have a variety of lesser consequences depending on, for example, the impact to downstream operations such as yield. Because of the structure of this approach, it may be necessary to provide for different levels of severity for some consequences in order to complete the risk analysis for all the possible threats.

If all the consequences and their ratings are acceptable to the SME team, then the risks can be accepted and the QRM exercise completed. However, continuation of the analysis to identify the likelihood of the consequence is usually warranted. The following step is intended to identify the threats or hazards that could cause the consequences identified in Step #1.

Step #2: Threat Evaluation

With the consequences identified, the next activity is to identify and understand what hazards, events, actions, or changes could cause the consequence. A brainstorming exercise by the SME team is usually required to complete this task. Usually, the consequence can be realized from several threats that may be external or internal to the process as initially defined. In order to identify these threats, the definition of the process may have to be expanded to include internal elements. For example, a particularly important threat may come from the failure of an instrument or subprocess within the initial process definition.

TABLE 2. Template concept for QRM exercise to manage enterprise threat risks.

QRM Threat Identification & Management Template

	A. Initial Risk Process Description (Step #1):		B. Risk Subject (Step #1 - What, Who):								
Unique Risk Sequence Number	C. Risk Consequence Impact Description (Step #1)	Consequence Index (Step #1) (C)	Initial Analysis & Evaluation (Step #2)				Mitigation Strategy w/Action Plan (Step #3)				
			D. Risk Threat Description	E. Process's Threat Vulnerability & Likelihood: Threat Knowledge & Process Vulnerability Description	E. Process's Threat Vulnerability & Likelihood: Initial Likelihood & Knowledge Index (U_T)	Initial Risk Rating ($C * U_T$)	F. Threat Reduction Strategy (New Process & Practices) and Revised Threat Uncertainty (U_T)	G. Process Control Stategy (New Process & Practices) and Process Propagation Uncertainty (U_P)	Revised Likelihood Index (U_T)	Revised Risk Rating ($C * U_T$)
1										
2										
3										
4										
5										
6										
7										
8										
9										

Depending on the scope of the QRM exercise, considerable effort may be required to evaluate and further define the process or processes to identify internal threats. An example is the expanded process network shown in **Figure 5**. The expanded process network may include additional definition of equipment components and inclusion of procedural processes used to control the unit operations.

After the process is further defined, a vulnerability analysis can be performed on the subprocesses to understand what vulnerabilities exist. A vulnerability analysis generally places a reduced burden on the SME team to assess uncertainties by focusing primarily on mechanisms by which the threat would propagate through the subprocesses to the output. Based on the vulnerability analysis, an approximate determination of the threat's uncertainty, in terms of likelihood, can be estimated.

To complete step #2, a likelihood index can be estimated. After the threats are identified, each threat can be evaluated from the perspective of the threat occurring and the likelihood that the threat will propagate through the process or sub processes to result in the consequence. Alternatively, as shown in **Table 1**, the knowledge level of the threat's impact on the process described in terms of the process's vulnerability to the threat is estimated.

Step #2 defines the following items in the analysis (see the template in **Table 2**):

D. Threat Sources — A definition of the threats, both internal and external, that might result in the consequence to the subject.

E. Process Threat Uncertainty — A description of the process's vulnerability to the threat and/or a rating of the knowledge about the process's likelihood of the threat resulting in the consequence. The initial likelihood/knowledge uncertainty index (U_I) is estimated by the team.

Once a U_I rating is estimated, the initial risk index can be calculated as the product of the C and the likelihood U_I. As shown in **Table 1**, a possible four-point scale for both indices is provided along with a 16-point scale for the overall risk index. At this point, the SME team may decide the risk is acceptable. If it is not, then Step #3 begins.

Step #3: Risk Mitigation

After the initial risk index has been determined, the unacceptable risks must be mitigated to an acceptable level before completing the QRM exercise. Risks are mitigated by either changing the existing system of processes or adding one or more new processes. In some cases, the process network identified in Step #2 may have to be further expanded. The process additions and/or modifications must be based on the SME team's understanding of the risk processes expanded to a level appropriate for the severity of the consequence. Frequently, a process map such as the one shown in **Figure 5** must be constructed to identify the various process elements along with the connections between the process elements. For most biotech UOs, procedural processes are required to set up, operate, and clean the equipment. These procedural processes can have a very significant impact on the operational threats associated with successfully operating the process step.

The Step #3 mitigation effort develops the following information (see the template in **Table 2**):

F. Threat Reduction Strategy — The uncertainty of the threat resulting in the consequence is modified by adding one or more new processes to reduce the likelihood of the threat reaching the core process elements. For example, if the threat is a contaminated raw material likely to result in the consequence, the addition of a new or enhanced screening process prior to the main process being evaluated will make it less likely that the threat could reach the key elements of the process. After the reduction strategy has been formulated, a lower likelihood of the threat reaching the process can be estimated as U_T.

G. Process Control Strategy — The process itself can be modified to decrease the likelihood that the threat can pass through the process. Frequently, the control systems used to control the process can be enhanced using the PAT principle to provide better control of the threat.[13] After the strategy is defined, a lower likelihood of the threat's propagation through the process can be estimated as U_P.

Determining the final likelihood (uncertainty) rating for (U_F) is evaluated by the SME team considering both U_T and U_P. Based on the team's judgment, the higher, lower, or some combination of the two uncertainty ratings, along with the C rating are used to define the risk's final index rating.

If the final risk index and evaluation does not meet the threshold for acceptance, further evaluation and analysis of the risk processes is carried out by the SME team to decrease the likelihood of the threat propagating through the process system. After Step #3, the final task of the SME team is to recommend acceptance of the risks to management.

Step #4: SME Team Acceptance

The remediated risk is accepted first by the SME team performing the QRM exercise and then by management, in the form of advancing the project. Part III of this paper expands the discussion of the complex decision to accept or further mitigate risks. Note that a key element in the final acceptance is also acceptance of the new and/or modified processes. The investment required to make the necessary changes can be significant, and rejection of the QRM exercise's results by the management team may be based as much on the size of the investment required for the risk's management as the consequence of the risk.

For important risks, the consensus of the greater risk analysis community appears to be that the final

decision-makers (management), should be a part of the SME team.[6] Only as a team participant can the decision-maker understand and appreciate the necessary give-and-take between the team members for ultimately making the SME team's recommendation. If a spreadsheet or table is used, such as the one shown in **Table 2**, it can provide significant documentation of the QRM exercise. However, for those who do not participate in the SME team's QRM exercise, it may not provide the high level of understanding required to make the correct decision.

Conclusion

Within the pharmaceutical industry, QRM is used for two purposes. The first is to assess threat risks associated with biomanufacturing processes and facilities. The second, which will be addressed in Part II, is to rank and prioritize process parameters based on their potential risk impact on the product's safety and efficacy on patients. Part I has emphasized the role of the process in assessing the impact of threats on producing a risk consequence to a predefined risk subject. By understanding the process, the threats can be mitigated by modifying the existing processes, or adding new processes to control or remove threats that might result in the risk's consequence.

References

[1] FDA (CDER/CBER) – *Guidance for industry: Q9 quality risk management.* June 2006. ICH. http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm073511.pdf

[2] Bernstein PL. *Against the gods: the remarkable story of risk.* Wiley & Sons, Inc., 1996. http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471121045.html

[3] Covello VT, Mumpower J. Risk analysis and risk management: an historical perspective. *Risk Anal*, 1985; 5(2): 103–120. http://dx.doi.org/10.1111/j.1539-6924.1985.tb00159.x

[4] Kahneman D, Tversky A. *Prospect theory: an analysis of decision under risk. In Decision, probability, and utility – selected readings*. Gärdenfors P and Sahlin N-E eds; Cambridge University Press, 1988.

[5] Kahneman D, Slovic P, Tversky A, eds. *Judgment under uncertainty: heuristics and biases*. Cambridge University Press, 1982. http://dx.doi.org/10.1017/CBO9780511809477

[6] Hubbard DW. *The failure of risk management: why it's broken and how to fix it.* Wiley & Sons, Inc., 2009. http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470387955.html

[7] Cox LA, Babayev D, Huber W. Some limitations of qualitative risk rating systems. *Risk Anal*, 2005; 25(3): 651–62. http://dx.doi.org/10.1111/j.1539-6924.2005.00615.x

[8] McDermott RE, Mikulak RJ, Beauregard MR. *The basics of FMEA*. Productivity Press; New York, NY, 1996.

[9] Carlson CS. *Effective FMEAs: achieving safe, reliable, and economical products and processes using failure mode and effect analysis*. Wiley & Sons, Inc., 2012. http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118007433,subjectCd-ST80.html

[10] Cox LA. What's wrong with risk matrices? *Risk Anal*, 2008; 28(2): 497–512. http://dx.doi.org/10.1111/j.1539-6924.2008.01030.x

[11] Ball DJ, Watt J. Further thoughts on the utility of risk matrices. *Risk Anal*, 2013; 33(11): 2068–78. http://dx.doi.org/10.1111/risa.12057 PMid: 23656539

[12] Aven T. *Quantitative risk assessment: the scientific platform*. Cambridge University Press; New York, NY, 2011. http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521760577

[13] FDA (CDER/CVM/ORA) – *Guidance for industry: PAT – a framework for innovative pharmaceutical development, manufacturing, and quality assurance*. Sept 2004.

[14] Witcher MF. A qualitative risk-benefit structure for developing and manufacturing biopharmaceuticals. *BioProcess J*, 2015; 14(3):4–12. http://dx.doi.org/10.12665/J143.Witcher

About the Author

Mark F. Witcher, PhD, Operations Lead, Strategic Manufacturing Concept Group (SMCG)

NNE, 1101 Slater Rd., Suite 120, Durham, North Carolina 27703 USA
Email: mkwh@nne.com | Website: www.nne.com

Mark is an SME related to process, business development, and operational issues associated with design, engineering, construction, validation, and operation of biopharmaceutical facilities. Previously, he was a consultant to the biopharmaceutical industry for more than 14 years on operational issues related to: process development, product development, strategic business development, clinical and commercial manufacturing planning, tech transfer, and facility planning, design, and construction. Prior experience includes executive positions with a CMO and a major biopharmaceutical company. Mark teaches a course on bioprocess process validation for ISPE.