Reprinted from
PHARMACEUTICAL ENGINEERING
THE OFFICIAL TECHNICAL MAGAZINE OF ISPE
JANUARY/FEBRUARY 2015, VOL 35, NO 1

www.PharmaceuticalEngineering.org

Risk Assessment: Issues and Challenges

by Joe Brady, PhD

This article presents an opinion and a perspective on the practical application of risk assessment, on how to adopt a scientific approach to the risk management process, and also informally dispenses some simple and pragmatic advice that may enhance a risk exercise.

Risk can be defined as the effect of uncertainty on objectives.[1] Risk assessment is considered to be the overall process of risk identification, risk analysis and risk evaluation.[2] The risk management process is the overall and systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.[1]

To be effective, the risk assessment and risk management processes both need to be properly understood, focused, transparent and clearly communicated. If a harmful event occurs, yet a risk assessment predicted that such an event was unlikely, everybody will want to know what went wrong. If risks cannot be properly evaluated, risk assessment itself becomes the biggest risk.[3] Therefore, the processes need assurances that they work.

A failed risk management process will inevitably leave a lot of questions to be answered, by the victims, those who were discommoded, or by the media. Types of questions asked will almost be universal. Who participated? Why were certain decisions taken? Why did it seemingly not work? Did anyone check the predicted outcomes before implementation? What confidence testing was done at the time to ensure that the assumptions were held to be true? These sound much like the same type of questions one would ask about a dubious scientific model.

This article is primarily focused on conducting an effective risk assessment, and then on the principles of risk review. Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyzes the risk in terms of consequences and their probabilities before deciding on whether further treatment is required.[2] Risk review involves reviewing the output and results of the risk management process to take into account new and ongoing knowledge and experience.[4]

Risk Management Process

Risk assessment can be considered a mechanism to unlock wisdom not yet experienced, upon encountering a new system. A typical risk management process, as per the hypothetical worked example outlined in Table A, is generally considered to broadly encompass the following sequence of activities:[1,4,5,6]

1. A team of subject matter experts creatively identify risks (faults/failures/hazards) associated with a new and unfamiliar system.
2. The identified risks are analyzed and evaluated. The acceptability of each risk is determined.
3. Risks that are considered unacceptable are treated by the selection of appropriate mitigation strategies that are both robust and cost effective. The mitigation strategies and controls themselves are analyzed and evaluated to affirm where residual risk is deemed acceptable. Suitable controls are subsequently implemented.
4. Risks are subsequently reviewed post system implementation. Every day that passes, every batch manufactured, every customer complaint received, all contribute to new

knowledge and this results in more experience with the now familiar system. The benefit of this now first-hand experience and wisdom not only assists with the identification of new risks, but also with the adjustment of the existing risk controls. New knowledge is used to keep the risk assessment current, relevant and robust.

Subject Matter Experts

Selecting a team of subject matter experts to participate in a robust risk assessment process is about ensuring that the

During the concept-phase* of a hypothetical project, an initial design specification is proposed and corresponding preliminary process flow diagrams and process descriptions are generated. The project team now take a risk management approach to assessing the robustness of the design specification, prior to the formal generation of user requirement specifications and the subsequent issuing to vendors with requests-for-quotations. The general sequence of risk management activities for this hypothetical scenario might look like the following:

Step #	Description
1	**Initiate the Risk Management Process, and Define Inputs**
1.1	The risk management facilitator is appointed.
1.2	**Input-1:** The objective of this particular risk assessment is four-fold: a. Ensure that critical process elements specific to product quality, patient safety and data integrity have been identified. b. Identify any opportunities for the implementation of technically sound improvements. c. Postulate a performance and functionality verification testing strategy focusing on the identified critical elements. d. Propose an appropriate and robust structure for the detailed design documents, so that they may be confidently used both for systems implementation and as the basis for developing robust verification test scripts.
1.3	**Input-2:** A team of subject matter experts is assembled and attends the risk assessment exercise. The team comprises of experts with both product and process understanding, and also of subject matter experts who are conversant in the applicable regulatory expectations and with the conventions of the company's internal quality management system.
1.4	**Input-3:** The above listed subject matter experts are made familiar with the project approach, contracts, project methods, cost controls, and project timelines.
1.5	**Input-4:** Descriptions of the manufacturing systems are presented to the team, as follows: • Unit operations and the integrated manufacturing process. • Intended clinical use of the product (pharmaceutical, medical device, or combinational product). • IT infrastructure, topology, components and system architecture, and an overview of the various functions of the range of software applications. • Proposed lifecycle documentation hierarchy (for specification, design and verification documents).
2	**Risk Identification**
2.1	The team is organized into multiple groups, in the interest of either grouping or balancing the presence of certain expertise within the individual groups.
2.2	The risk statement/problem/enhancement is unambiguously communicated by the facilitator to the team, and is based on potential manufacturing system failures that could negatively impact on product quality, patient safety and data integrity.
2.3	During the risk identification phase, each team identifies potential faults (risks/failures/hazards) associated with the manufacturing systems, using creative fault finding tools, based on individual and combined subject matter expertise.
2.4	At the end of the risk identification phase, the facilitator collects the list of risks generated by each team. In this hypothetical scenario, the facilitator transcribes and collates a combined list of one hundred and thirty (130) faults into a risk identification report. Typically there will be significant overlap between observations amongst the various groups, so eventually the facilitator whittles down the overall list to one hundred (100) unique faults. Now a list of one hundred faults exists, the next step is to analyze and evaluate them.
3	**Analyze and Evaluate Risks**
3.1	Here the team starts with a list of one hundred identified faults. Remember, it will always cost time, money and resources to mitigate against a risk. Straightaway, it is obvious that all the faults cannot have the same priority (it would be unusual if they did). The next step now is to analyze and evaluate each and every fault and rate them against one another so that they can all be arranged in some order of priority. At a minimum, it is recommended to assign a risk-score to each fault based on the estimated product of the probability-of-occurrence and the severity of that occurrence should it occur (other categories could be included to finely-tune the priority order, such as assigning values for GxP impact, complexity, novelty, GAMP® software and hardware category, and detectability, for example).
3.2	The list of the one hundred identified faults is now rearranged, where the higher priority faults are organized towards the top of the list, and with the lower priority faults at the bottom. Ultimately, the priority order is in the context of product quality, patient safety and data integrity.
3.3	Now risk acceptability decisions have to be taken. A risk-acceptance line needs to be drawn in somewhere on that list. Below that line are the potential faults that the team can currently accept and live with. In other words, they are satisfied that the probability of occurrence is so low that the event might never be experienced over the lifecycle of the system, or that they would be able to recover relatively unscathed should the event ever occur in the first place, or both. Above that line, however, the risk-score is deemed to be too high, and thus unacceptable. For the prioritized faults above the line, risk control and treatment strategies will now have to be devised to reduce the risk-score to a more acceptable residual level. This will require a design change or a procedural change, or both. In this hypothetical scenario, the team decides that seventy (70) of the faults fall below the risk-acceptance line, with thirty (30) remaining above. The team now needs to decide upon creative risk controls and treatments for these top thirty high priority faults.

Table A. Example of general sequence of activities associated with a typical risk management process.

right questions are put to the most appropriate and competent individuals. Where a risk assessment goes awry in the pharmaceutical industry, the obvious questions from the regulatory authorities might include: Where was the design and development team? Were any test engineers or validation specialists involved? Where were the manufacturing teams such as operations, utilities and facilities? What about the whereabouts of packaging and labelling representa-

Step #	Description
4	**Risks Control and Treatments**
4.1	The team has a priority list of thirty unacceptable faults. The team now wishes to revisit and update the initial design specification and preliminary process flow diagrams and process descriptions.
4.2	Here the team creatively devises a number of control and treatment strategies for each fault. Remember, there will most likely be multiple possible solutions to correct every fault.
4.3	With multiple options now available, the next step is for the team to evaluate each and every option in terms of robustness and cost, and impact on the project schedule.
4.4	Once suitable options have been selected to correct what was initially deemed as thirty unacceptable faults, the team now has to re-assign a risk prioritization score and evaluate the residual risk. Hopefully, the new risk prioritization score will drop that particular hazard well below the risk-acceptance line on the original list (from Step-3.3, above). If it does, all well and good. If it doesn't, more options may need to be considered to further mitigate the problem until acceptable residual risk level is achieved, or a business decision may need to be taken to proceed or not proceed with the project in its current guise.
4.5	Assuming that suitable control and treatment strategies have been decided upon for the all thirty faults, the next step is for the team to implement the various options. This should lead to an updated design specification, along with the corresponding process flow diagrams and process descriptions.
5	**Risks Report, and Outputs**
5.1	A summary report of this risk-assessment exercise is written up, listing at a minimum the background to the exercise, the overall objectives, the list of attendees and all other inputs, the methods used to identify faults, and the all-important list of outputs.
5.2	**Output-1:** The first output is arguably a comprehensive list of identified critical process elements specific to product quality, patient safety and data integrity. A rationale should be included for each element as to why it is considered critical.
5.3	**Output-2:** A primary output for this risk assessment exercise is the updated design specification, and corresponding process flow diagrams and process descriptions. Decisions to update the specifications and implement technically sound improvements should be traceable to the faults being remediated, and the associated control and treatment strategies selected. All specification update decisions must be obvious, traceable and fully informed, and should ultimately be shown to result in clear and unambiguous enhancements to patient safety, product quality, and data integrity.
5.4	**Output-3:** Robust user requirement specifications can now be confidently generated and issued to the vendors with requests-for-quotations. The specific critical process elements should be clearly articulated for the appropriate vendors, so that they might best understand how best to prepare their proposed functional solutions.
5.5	**Output-4:** With all critical process elements identified and with robust user requirements now in place, the team can immediately start with planning an efficient validation strategy, beginning with generating integrated performance level verification tests.
5.6	**Output-5:** During the project phase,* once the vendors submit their proposed functional design solutions and the vendor selection process is complete, the team can immediately begin planning and generating functional and unit-operation verification tests. This can then influence the structure and layout of the vendors' detailed design documents, so that they may be unambiguously used both for systems implementation and as the basis for developing robust verification test scripts whilst maintaining a focus on the critical process elements.
6	**Risk Review**
6.1	Achieving compliance and fitness for intended use is the ultimate goal of the various risk management processes. But how does the team know that their risk management approach works? Across the entire systems lifecycle phases(*) there will be multiple opportunities for the application of risk-based decision making. Each and every risk assessment in sequence should reference and build upon the assessments that have gone before. A common sense, and non-onerous, administrative approach should link the various outputs of the evolving program of risk management exercises, and encourage a system of checks and balances amongst iterations.
6.2	As more experience is gained across the lifecycle, the resulting knowledge may lead to the identification of new critical process elements. Indeed this new knowledge could even lead to the downgrading of earlier identified critical process elements, with justification.
6.3	Ongoing system performance monitoring, incident management, corrective and preventive action and repair activities can intuitively be linked to evolving and iterative risk management exercises. This should result in continuous opportunities for the identification of technically sound improvements, more smart and intelligent verification testing, and maintenance of specification and design documents.
6.4	The risk review process can also be inextricably linked to the outputs and observations from both ongoing internal and external audits of the installed and implemented system.
*Reference Figure M3.3 from GAMP® 5, for an overview of the typical use of risk-based decision making across the system lifecycle.[7]	

Table A (continued). Example of general sequence of activities associated with a typical risk management process.

tives? Did the quality assurance and quality control teams contribute? Did any personnel associated with warehousing and distribution, and product monitored post-implantation play a part? Was there a need for healthcare professionals to participate?

What influences the decisions when selecting a team of subject matter experts to partake in a risk assessment process? Everyone has expertise on a plethora of subjects, but the actual degree of expertise in each case varies. The point here is that everyone could potentially contribute to nearly all risk assessments in the work place. Being selected or choosing to participate is primarily influenced by the extent of one's expertise. The risk assessment process is initiated with a clear and unambiguous problem statement, together with a clear study context. A crucial query for the risk assessment team at this point is who they would ideally like to have in attendance to brainstorm on the problem. What expertise would best contribute to the study?

The team organizing the risk assessment need to, with great dignity, determine the optimum degree of expertise available within the organization. Sometimes they may need to look outside their industry for a suitable degree of subject matter expertise. The organization needs some novel communication tools to let the employees know what risk assessments are currently being conducted, and those that are planned for the future. The presumption here is that all employees would enthusiastically be willing to contact the risk assessment team should they feel that they could contribute constructively to a particular exercise. The organizing team ought to remember to preserve dignity at all times, and respect all submissions and volunteers. If a volunteer at this point-in-time is not optimum for a study and is not selected, the chances are that at some point in the future they will be suitable for another. Nobody should ever feel discouraged before or after volunteering, regardless of it being their first time or not. The organizing team should be forever grateful and humble when someone offers to share the extent of their expertise. Everyone generally looks forward to sharing their knowledge in a collaborative and encouraging environment, and they need to be respected for this each and every time.

Perhaps, a novel user-friendly database of skills and expertise could be formally or informally maintained by the organization, and in particular be updated by the individuals themselves. The risk assessment teams would have access to this database which may help them identify key individuals for a particular study. Too often, individual expertise is completely overlooked in the workplace due to its invisibility, and such a database might be a contributor to making it more noticeable. The risk assessment team needs to be aware of any strong individual biases or ardent views that may skew the study, and try to carefully balance these out among the selected contributors. Different personalities and cultures are more assertive than others when it comes to declaring individual expertise. In this instance, a method may be needed so as to gently coax out individual strengths from the more introverted participants.

Finding Faults

There seems to be only one guarantee with risk assessment and that is all the risks will never be identified. Similarly, when a fault is identified it is not usually possible to identify all causes, so therefore total treatment and mitigation is seldom a reality. The most crucial ingredient to finding faults is to have the correct subject matter experts doing the brainstorming. Experienced and/or knowledgeable personnel thinking on the problem is a prerequisite. Risk assessment is used to identify potential hazards in advance, and subsequently put some treatments and mitigating safeguards in place to prevent the causes of their likely occurrence. Risk assessment can be considered an important supporting process to the product lifecycle.[7,8] This lifecycle support contributes to progressing innovations from design through to eventual implementation with the intent of manufacturing and distributing a safe and effective product.

The first stage of a risk assessment process is generally considered to consist of the creative identification of risks (faults/failures/hazards). Hopefully, the use of systematic tools will facilitate the participating subject matter experts to methodically, logically and objectively make risk observations. This stage of the risk assessment process requires intuition and creativity, and any or all of those practices that actively stimulate and promote intuition and creativity. It is about creative fault finding. Innate creativity is something that can be facilitated using systematic tools. Everyone has the capacity to be creative, but the conditions need to be suitable for it to manifest. Creative fault finding requires an enabling, stimulating, encouraging, challenging, and inspiring environment.

The risk assessment process is initiated with a problem statement and a study context. The desired subject matter expertise is ascertained and the relevant experts are selected to participate. The appointment of study facilitator should be given serious consideration. Ways to creatively stimulate the identification of faults should be developed. For example, a prototype may be presented, a mock-up built, or a computer model generated. Systematic risk assessment tools need to be selected to assist with, and drive forward, the brainstorming of faults.[2,5] These can be used either in a standalone capacity or adapted and combined for maximum flexibility.

Risk serves as a stimulant. When faced with something new in life, people tend to extrapolate past learnings, wisdom and experience, and apply it intuitively to any new system to try and predict where hazards might arise. Indisputably, many skills and proficiencies are immediately transferable between systems and industries. First and foremost,

intuition based on experience is central to identifying faults associated with a new and unfamiliar system. People can be emotional, impulsive, and at times can be somewhat predisposed to identifying arbitrary faults. Emotional impulses can be fuelled by, for example, fear, pride, prejudice, insecurity, or envy. These can lead to substantial and haphazard biases in people. Ideally, a good risk assessment process with systematic tools will help a participant to recognize and neutralize their own biases – both positive and negative – leading to methodical, logical and objective fault observations.

Fault Tree Analysis (FTA), cause and effect (Ishikawa/fish-bone) diagram, Preliminary Hazard Analysis (PHA), and Event Tree Analysis (ETA) are very intuitive systematic tools to identify faults with. They are relative easy to learn and to become proficient at using, and be systematic in their application. Another useful technique for finding faults is based on the first of the seven steps of the Hazard Analysis and Critical Control Points (HACCP) technique. The first step of HACCP is to conduct a hazard analysis for each step of a process and find faults based on a process description and on a straightforward high-level visual review of a process flow diagram (the first step of HACCP also includes the determination of preventive measures associated with the identified faults).

Hazard and Operability Analysis (HAZOP) tools can be used to identify operational faults as a result of deviations from design intent. The HAZOP tool is very structured and formal. It can be very time consuming and resource-heavy, and it may take the team a little time to master how to use it effectively. The Failure Mode Effect Analysis (FMEA) tool is used to determine causes and effects of pre-established faults. A range of faults must first be established (using one of the earlier tools described above, for example) and inputted into the FMEA spreadsheet. The spreadsheet technique will then facilitate the brainstorming of related causes and effects. Training a team of individuals how to use FMEA effectively and consistently can be a bit of a challenge. The FMEA team may have a tendency to deviate on tangents outside the frame of reference for the study, so it is perhaps important that a FMEA study be carefully coordinated by the appointment of a facilitator.

For fault identification purposes, FTA, cause and effect diagrams, PHA, ETA and HACCP can be deployed and used throughout all the lifecycle phases of a manufacturing system (see GAMP® 5 for a description of the lifecycle phases.[7]) They are particularly effective during the earlier phases of a project, such as the concept, planning and the functional-design-specification phases where there is limited information on design details or operating procedures. Often the outputs from these studies act as a precursor to further studies, such as FMEA; however, both HAZOP and FMEA can be considered particularly formal, time consuming and resource-heavy tools. Both are perhaps best used during the detailed design phase of project, prior to a design being official issued for construction.

During the risk assessment process, equal importance should be allocated to everyone's views. The facilitator may find themselves constantly moderating the forthright individuals, while at the same time patiently encouraging and coaxing contributions from the more timid characters. Robust debate is encouraged to refine ideas, but a culture of 'respect for all' must prevail. The momentum between the introverts and extroverts on the team must be balanced and fair. Fault finding is not a competitive sport, and it is quality over quantity every time.

During a risk assessment, groupthink should be eliminated as much as possible as it can lead to biases and irrational decision making. In a respectful and tactful manner, the potentially destructive effects of company hierarchies also must be minimized. The hierarchical perception of 'the boss is always right' can have an inhibitory effect on creative flow throughout the entire risk assessment process. If their ideas remain unchallenged, submissive conformity may lead to substantial biases in the overall process and invariably skew the resultant model. Certain cultural sensitivities may require, or leave no other option than to, segregate and group hierarchies according to their status and rank, where each organizational level embarks upon their own separate risk assessment process.

Everyone should be encouraged to participate in the process to the fullest possible extent. Individual thoughts and knowledge are only useful when they are shared. Concepts evolve, expand and flourish with robust debate. Without the entire team dynamic, the foundation of many ideas would simply not transpire; therefore, no one individual can ever lay exclusive claim to an idea. The facilitator should collate and combine all identified faults into a logical preliminary report that compliments the study question. The risk assessment process may then proceed to the next stage, where the team of subject matter experts will now analyze and evaluate the risks. It may be a good idea for the team to have a rest or recreational period before progressing into this next stage, so that they might recharge their creativity energy.

Analyzing and Evaluating Risks

Once a list of risks is available, they can now be analyzed and evaluated with respect to one another. The acceptability of each risk is determined. Which are the risks that are tolerable? Which are the risks that are not tolerable and require treatment? One way to do this is to compare one risk against another and come up with some type of ranking system.

A traditional ranking system for risks is based on the product of probability and severity. Here a quantitative value or qualitative hierarchy is assigned to each risk based on the probability of their likely occurrence, coupled with the severity of that event should it occur. The risk assessment team

will probably always feel that they do not have enough information to assign a probability and severity value or establish a hierarchy. A complete information set, regrettably, will most likely never exist; therefore, every judgment will only be an estimation based on the limited information at hand. This is usually a good enough place from where to start the risk assessment process, and commence formulating the risk evaluation model. Assurances that the evaluation model is effective will be based on a continuous iterative risk-review process.

For both probability and severity, quantitative point-scales are often used, with the scale one to five (1-5) getting frequent usage. The value for both probability and severity are multiplied together to give a risk score. Simple stratification methods are often used. These typically use red-yellow-green or low-medium-high rating scales so that risk likelihoods can be displayed on a two-dimensional heat-map[3,7] (see Figure M3.5 in GAMP® 5 for an example of a heat-map.[7])

Severity, for example, in the pharmaceutical industry is generally in the context of patient harm. Descriptors for severity might include: 1. low, medium or high, 2. minor, critical, major or catastrophic, and 3. worry, acute illness, hospitalization or death. Once a range of risks has been identified, a relative severity rating is assigned in the context of the overall risk question. If a risk is determined as fatal, that severity cannot be reduced by treatment. However, what can be done is to reduce the probability of that risk occurring in the first place, by the implementation of suitable treatment and mitigation strategies.

Descriptors for probability might include: 1. very low, low, medium, high or very high and 2. frequent, probable, occasional, remote or improbable. In many instances there may be no scientific or statistical basis on which to form any calculable probability whatsoever. However, there is more to assessing risk probability than statistics.[9] A risk assessment is not an attempt to precisely establish absolute probability from the onset, but like the severity rating, merely to rate a predicted risk against another in the context of the specific risk question. For example, two separate studies with seemingly unrelated contexts may identify the same type of risk, but there is no guarantee that the risk will be assigned the same relative probability rating. The rating of one risk is relative to the others identified in the same study, and is context specific. It may not be a good idea to carry probability determinations from one study into another. Perhaps as various risk evaluation models mature, one may indeed be able to build up a general rating system for common risks that may be exchangeable between various studies. Probability and severity ratings, although subjective, are relative in the context of a specific study. Risk practitioners need to be careful, as momentum can be lost if the teams get mired down in making these determinations, particularly in the case of probability.

Risk Control and Treatment

The idea for the implementation of one or more control and treatment actions is that it may stop a trigger event from causing a fault in the first place.[9] Risk treatment, according to ISO 31010, can involve:[2]

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties
- Retaining the risk by informed decision

Additional control and treatment measures typically employed by manufacturers include:[5]

- Eliminating the risk completely
- Substituting one thing with another that is more acceptable (substitute one solvent for another)
- Uncoupling, loosely coupling, or modularizing a process to prevent a problem from escalating and impacting on an entire process (confine an event to a single unit operation)
- Applying engineering controls (automation interlocks)
- Isolating a process or product to prevent contamination, and/or protect operators and the environment from accidental exposure
- Providing information (drug contraindications on the container and on the patient leaflet)
- Validation (for example, providing documented test evidence of the robustness of all the cold-chain management steps for a temperature sensitive vaccine formulation)
- Duplicating the asset (having two smaller production sites instead of just one large one, in case one site has a catastrophe)
- Proceduralizing a process by providing specialized information
- Training as both a preventative and protecting control measure
- Monitoring a process to identify an event and initiate appropriate controls

Risk Review

It is somewhat obvious lately that risk assessment doesn't always work, leaving behind a regrettable aftermath of devastation, loss and human hardship. Financial institutions lose money regardless of their complex multivariate risk algorithms devised by physicists and mathematicians. Defenses to natural disasters are breached because levees and sea-walls are simply not tall enough or strong enough

to withstand rare storm surge or tidal wave events. Unusually, civilian aircraft are confronted with the hazard of not being diverted away from conflict zones and are left susceptible to a military strike. Therefore, a continuous, weary and conspicuous eye should be cast over each and every risk evaluation and risk based decision.

ISO 31010 recommends that monitoring and performing reviews should be established as part of the risk management process. Risks and controls should be monitored and reviewed on a regular basis to verify that:[2]

- Assumptions about risks remain valid.
- Assumptions on which the risk assessment is based, including the external and internal context, remain valid.

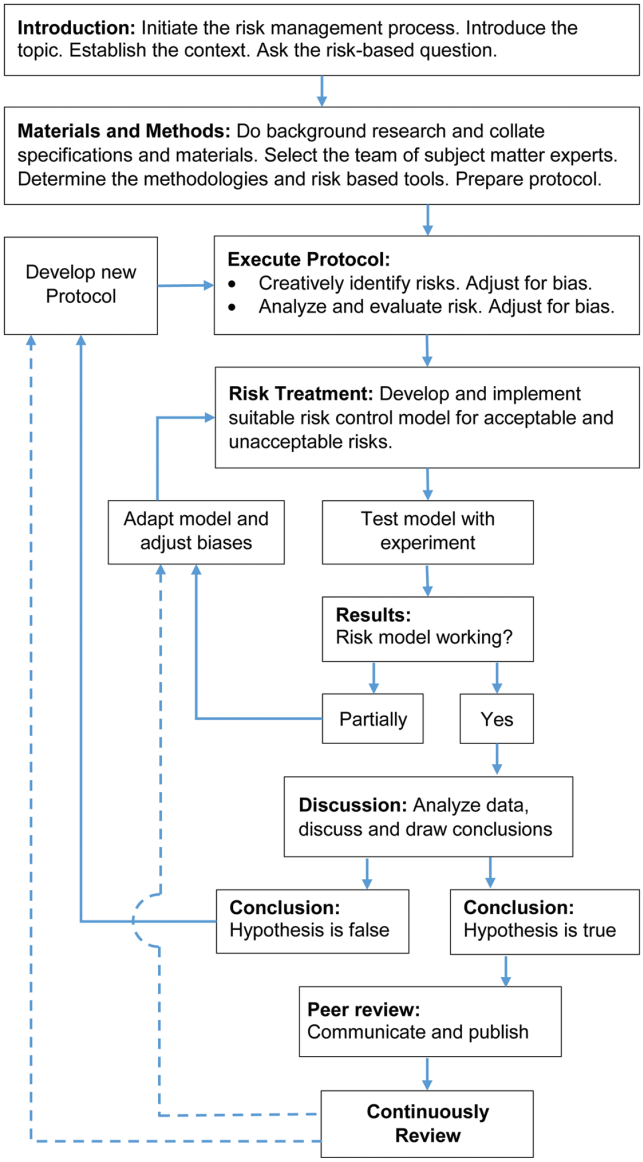

Figure 1. Application of the scientific method to the risk management process.

- Expected results are being achieved.
- Results of risk assessment are in line with actual experience.
- Risk assessment techniques are being properly applied.
- Risk treatments are effective.

Application of the Scientific Method to the Risk Management Process

Instinctively, resultant risk treatment and mitigation strategies will never be fully trusted, nor should they be. The point here is that risk analysis and evaluation is not supposed to be a one-time event. To say that a documented risk-based decision was taken once upon a time, and now the probability of hazard occurrence is under control is simply not true. The assumption that a once-off risk assessment resulted in hazard consequences that are indefinitely tolerable is false. An effective risk evaluation model should ultimately lead to logical and traceable decisions regarding ongoing treatment and control of potential risks. But like all models it needs to be proven that it actually works. This is what any competent authority will expect if they are presented with a risk based decision. Science purports to assist the risk assessment process, so therefore one must, like all good scientific investigations, ensure the risk evaluation model robustly holds true within the context of the study question.

A risk evaluation model, perhaps, should be treated the same way as a model derived from the scientific method, as illustrated in Figure 1. Generally the scientific method begins with replicate experiments with controlled inputs to yield consistent observed outputs. This empirical output data is assessed and formulated to reveal novel correlations. The correlations are modelled to explain the empirical observations. Based on theoretical inputs, the corresponding outputs are then predicted using the model. To prove the validity of the model, replicate experiments are executed using the same theoretical inputs. The resultant empirical outputs are then compared against the predicted theoretical outputs. The robustness of the model is forevermore challenged and modified based on endless inputs and observed outputs. The same philosophy should hold for risk evaluation models in order to prove the risk assessment hypotheses is true.

Conclusion

Risk assessment is a method for the systematic analysis of uncertainties on the objectives of an organization. It is a creative process that must be both facilitated and stimulated. In an organization, a culture of engaging with and including everyone in the risk management processes should be developed. Every organization has numerous experts on all sorts of specific risks, and chances are that many of them are not in management. Some effort ought to be made to survey representatives at just about every job level in the firm, in terms

of contribution.[3] The risk management process cannot take place in isolation, but needs to be supported by a culture and framework within the organization.[6]

The golden rule of any risk evaluation model should be to simply make sure that it works. Always have a healthy obsession with acquiring good quality data and evidence, using good scientific practices, to support the hypothesis that it does work. Examine any evidence objectively before making any judgment or decision. Recognize biases in order to make better decisions, and challenge all preconceptions (in a professional, diplomatic and sensitive way).

To paraphrase Peter L. Bernstein,[10] show the world how to understand risk, measure it, and weigh its consequences, then convert risk-taking into a prime catalyst to drive innovation.

References

1. ISO 31000, *Risk Management – Principles and Guidelines,* International Organization for Standardization, Geneva, Switzerland, 2009, www.iso.org.

2. ISO 31010, *Risk Management – Risk Assessment Techniques,* International Organization for Standardization, Geneva, Switzerland, 2009, www.iso.org.

3. Hubbard, D. W., *The Failure of Risk Management: Why It's Broken and How to Fix It,* John Wiley & Sons, Inc., 2009.

4. *ICH Q9 – Quality Risk Management,* International Conference on Harmonisation, Geneva, Switzerland, 2005, www.ich.org.

5. Vesper, J.L., *Risk Assessment and Risk Management in the Pharmaceutical Industry – Clear and Simple,* PDA/DHI, 2006, www.pda.org.

6. Hopkin, P., *Fundamentals of Risk Management – Understanding, Evaluating and Implementing Effective Risk Management,* Kogan Page Ltd., 2012.

7. *ISPE GAMP® 5: A Risk Based Approach to Compliant GxP Computerized Systems,* International Society for Pharmaceutical Engineering (ISPE), First Edition, January 2010, www.ispe.org.

8. *ASTM E2500 – Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment,* American Society for Testing and Materials, 2007, www.astm.org.

9. Fenton, N., and Neil, M., *Risk Assessment and Decision Analysis with Bayesian Networks,* CRC Press, Taylor & Francis Group, 2013.

10. Bernstein, P.L., *Against the Gods – The Remarkable Story of Risk,* John Wiley & Sons, Inc., 1998.

About the Author

Joe Brady is the Director of Global Compliance and Validation at Zenith Technologies. He has more than 17 years of project experience in the pharmaceutical, biopharmaceutical and medical device industries in Ireland, Singapore, China, the Netherlands, France and the USA. Brady is also an assistant lecturer with the Dublin Institute of Technology (DIT), Ireland, in the School of Chemical and Pharmaceutical Sciences. He lectures on the Masters programs in "Pharmaceutical Validation Technology" and "Pharmaceutical Quality Assurance." He can be contacted by email at: joe.brady@zenithtechnologies.com or joe.brady@dit.ie.