Handling the Truth in Risk Management

Kevin M. Curran and Michael W. Curran

ABSTRACT: A successful risk management program requires commitment on the part of the analysts and the decision makers. This commitment must begin with a reliable risk analysis methodology. Given a reliable process, however, managers and other decision makers must come to grips with the analysis results - regardless of how favorable or unfavorable they may be. Decision makers who use risk analysis merely to determine contingency requirements (or other necessary adjustments to any budget) will never capitalize on the real power of a sound risk analysis process - the insight and direction it provides to favorably impact the future. Those who finally reach acceptance, will find they have a powerful tool to improve their organizations' (and their own) bottom lines. All of this reduces to one simple question for decision makers and risk analysts alike: "Can You Handle the Truth?"

KEY WORDS: Risk analysis, benchmarks, contingency, owners, and project management

The 1992 movie, "A Few Good Men," included a courtroom scene with memorable dialogue between the witness, Colonel Nathan Jessep (Jack Nicholson) and the opposing attorney, Lieutenant J.G. Daniel Kaffee (Tom Cruise):

Jessep: You want answers?
Kaffee: I think I'm entitled to them.
Jessep: You want answers?
Kaffee: I want the truth!
Jessep: You can't handle the truth!

That dialogue characterizes the chasm that can exist between seasoned risk analysts and their decision maker clients. The disturbing fact is that in many cases decision makers simply cannot handle the truth! This article, based on decades of practical experience, describes the reasons why implementing a reliable risk management program is often a significant cultural challenge.

Do you want more risk in your life? Your initial response to that question was likely an immediate and resounding, "No!" To most people, the word "risk" implies undesirable potential outcomes - not desirable ones. After all, risk is a four-letter word!

Based on that observation, it would seem that the word risk is unambiguous. Not so. For example, use of the word may imply desirable, as well as undesirable, potential outcomes (e.g., "upside" risk as well as "downside" risk).

AACE International's Decision & Risk Management Committee struggled with such matters in its development of the **AACE International Risk Management Dictionary**, a project that involved over one hundred managers and professionals both from within and outside of the cost engineering and project management communities. The project took over three years to complete.

The major unexpected outcome was the inability of these practitioners to agree upon one definition for the word risk. It was finally agreed that the dictionary would include three such definitions along with the admonition that authors writing for publication in AACE International media should state how they define risk or else refrain from using the term in their works. (The authors will abide by that directive in the rest of this article.)

AACE International is not alone in dealing with this problem of terminology. Other professional organizations continue to debate the definition of risk. The resulting multiplicity of definitions not only fosters confusion within risk management ranks, it also affects communications with decision makers.

Most decision makers (and most people in general) perceive risk as something to be avoided. Why else do they speak of reducing risk rather than also increasing it? The importance of selecting the best definition of risk cannot be overstated. The use of appropriate terminology is one of the fundamental cultural challenges facing risk analysts when dealing with decision makers.

Today, many organizations have chief information officers (CIOs). That was not always the case. For many years, information technology (IT) managers were not positioned in the highest levels of most organizations. The reason was not simply a lack of appreciation for the strategic power of IT. A key obstacle was that IT professionals often discussed issues in IT terms rather than in the language of management—plain English or other native tongue. This issue was the subject of articles that appeared in the early 1980s in several information management periodicals. For the most part, it seems that IT professionals have learned this valuable lesson.

Today, risk management professionals face a similar challenge. Recently, for example, a board of directors voiced displeasure at the use of technical jargon by a risk analyst during his presentation of results for a capital project. Later, that same board of directors had kudos for the replacement risk analyst who chose to use commonly understood definitions for terms such as risk. With few exceptions, decision makers do not want to be confronted with such esoteric concepts as sampling theory, asymptotes, and kurtosis (a term that sounds more medical than statistical).

A sound risk analysis is useless if the analyst can't communicate the results in everyday business terms rather than statistical or engineering jargon. Simply put, decision makers are there to make decisions. They are not there, nor do most desire, to be trained in risk management or statistical terminologies or methods.

Before any risk management program can be successful, risk management professionals must recognize that, in their communications, decision makers are best served by words and definitions that conform to everyday usage. Only then will risk management be given its rightful place in the corporate lineup alongside IT and other strategically important functions. This is already occurring to a limited degree. A number of organizations have created the position of "CRO" (chief risk officer). However, such positions are often filled by experts in insurance, claims and the like rather than in broad risk analysis and risk management skills.

With risk considered an unfavorable entity, "opportunity" can be defined as its

favorable counterpart. "Uncertainty" can then be defined as the combination of both risk and opportunity. This relationship can be represented as: Uncertainty = Risks + Opportunities. (This terminology is consistent with the guidance provided in **AACE International's Risk Management Dictionary** and will be applied throughout the remainder of this article.) Accordingly, the term risk management is understood to mean "risk and opportunity management" and risk analysis as "risk and opportunity analysis."

This is but another example of the power of words. By mentally appending the words "and opportunity" to the word "risk," we are constantly reminded that the term "risk management" deals with two distinct entities: risk and opportunity. Failure to understand this can result in a special form of risk—that which is incurred when an opportunity is not surfaced and capitalized upon! A simple and readily recognized acronym can help to keep this importance in mind: ROI. No, not "return on investment." In this case, ROI stands for "Risk and Opportunity Investigation."

There is an abundance of reference material covering, in varying detail, how risk analysis should be performed. Often technical in nature, such publications typically fail to address the primary challenge of instituting a successful, quantitative risk analysis process: the mindset of the decision team.

In many cases, the failure of an organization's quantitative risk management function to achieve its full potential originates from its results being mistrusted, misused, abused, or ignored. Practical risk analysis experience, gained from conducting thousands of analyses over a period of 40 years, supports the following observation: decision makers and the professionals who support them must progress through several mindset changes before a successful risk management program can spring forth and blossom.

What is a successful risk management program? It is one in which the analyses predict actual outcomes with acceptable reliability and one that is trusted by decision makers. However, acceptable reliability alone does not bestow trust. Other factors are in play.

Obviously, decision makers cannot put their trust in a risk analysis process until it has been proven reliable enough to earn that trust. But, even with reliable and proven risk analysis practices, decision makers must first overcome psychological challenges before trust can be instilled and the full power of such practices realized.

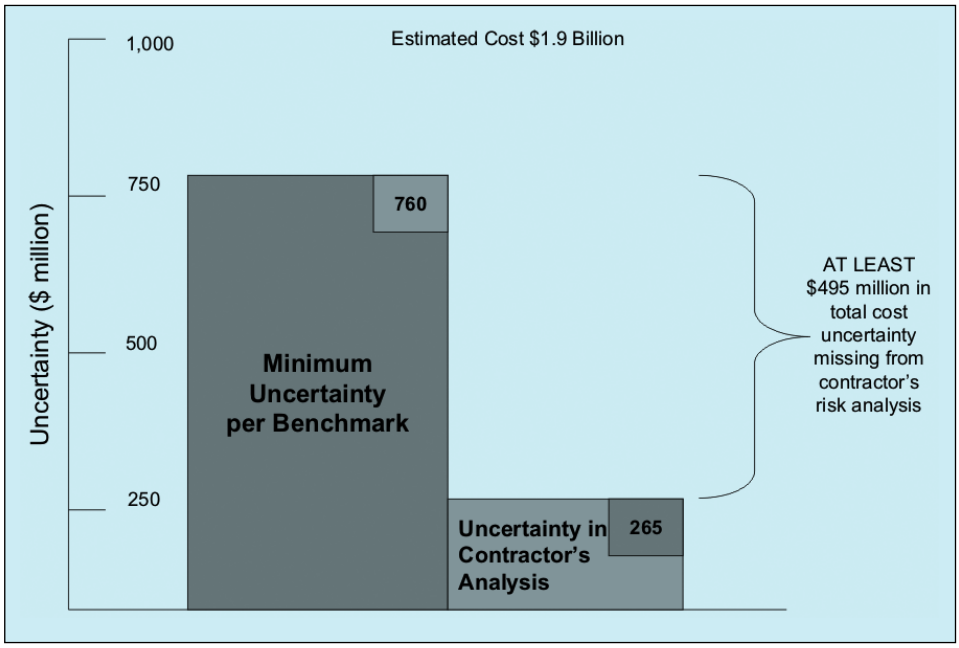

Figure 1—Uncertainty Benchmark

This article describes some of the details regarding those psychological (i.e., mindset) challenges and real-world examples of how they have both hindered and helped decision makers. The importance of overcoming these challenges cannot be understated when attempting to implement a sound risk management program.

Similar to the well-known stages of personal grief, the stages of the risk management mindset are readily identifiable, and include the following.

The Five Stages of the Risk Management Mindset

- fear;
- simplification;
- denial;
- anger; and,
- acceptance.

Fear

Fear of making a wrong decision is the stimulus that prompts decision makers to consider risk management in the first place. This can be an individual fear, an institutional fear, or both.

Individual fear is the concern a decision maker has that a wrong decision will lead to personal loss (loss of prestige, political capital, a bonus, promotion to a higher position, etc.).

Institutional fear is the concern, throughout the organization, of an entity-level loss (loss of shareholder value, loss of return on capital, etc.).

In most cases, both forms of fear lead decision makers to risk management in order to improve their chances of making good decisions. Without fear, of course, decision makers and organizations would move forward with their original plans without concern for their outcomes.

Simplification

Simplification relates to decision makers and, in some cases, risk analysts applying simplistic approaches to preparing risk analyses and/or interpreting them. Simplification can take several forms including: assuming that job or industry knowledge equates to risk analysis knowledge, assuming that analyzing multitudes of elements in plans improves results (i.e., the simplistic assumption that "more is better"), assuming that one-on-one interviews provide reliable risk analysis input data, assuming lump sum contracts always reduce uncertainty, etc. The ultimate simplification is often heard expressed: "We'll keep things under control by working harder and smarter." This strategy may work of course if we have been lazy and stupid in the past!

Denial

Denial is the outright dismissal of risk analysis results. In other words, the results are ignored because they do not conform to the decision maker's perceived level of

uncertainty in the decision. A decision maker might perceive that there is more uncertainty in the project or plan than is indicated by the risk analysis results. In most cases, however, the opposite is true: decision makers tend to perceive less uncertainty than is indicated by the results of the analysis.

Anger

Anger surfaces when the decision maker not only disagrees with risk analysis results (denial) but attacks the risk analysis process or the facilitator's methods. In many cases, this occurs because the decision maker is concerned that the risk analysis results will be shared with those in superior positions and the decision maker's competence might be called into question. Anger is typically directed at the risk analysis results, the risk analyst, the decision team (those who provided the input data), or any combination of these "targets."

Acceptance

Acceptance appears when the decision maker not only trusts the results of the risk analysis but readily commits to executing risk mitigation and opportunity capturing options.

For example, the engineering division of a large metals company distrusted the results of the risk analysis process that was being introduced into the organization. Months later, engineers within the company would not provide final estimates to corporate headquarters unless risk analyses were first conducted. The analysis process had proven its reliability over its initial period of use and the engineering group did not feel comfortable providing final estimates to top management without first having those estimates evaluated for their inherent risks and opportunities. They began to put their trust in the process and gained substantial improvements in capital effectiveness.

One or more of the five stages of mindset appear in some degree during virtually all risk analyses. The following are some examples of how these stages have surfaced during real-world analyses of projects and other business plans.

Some Real-World Examples

(All monetary values are stated in US dollars.)

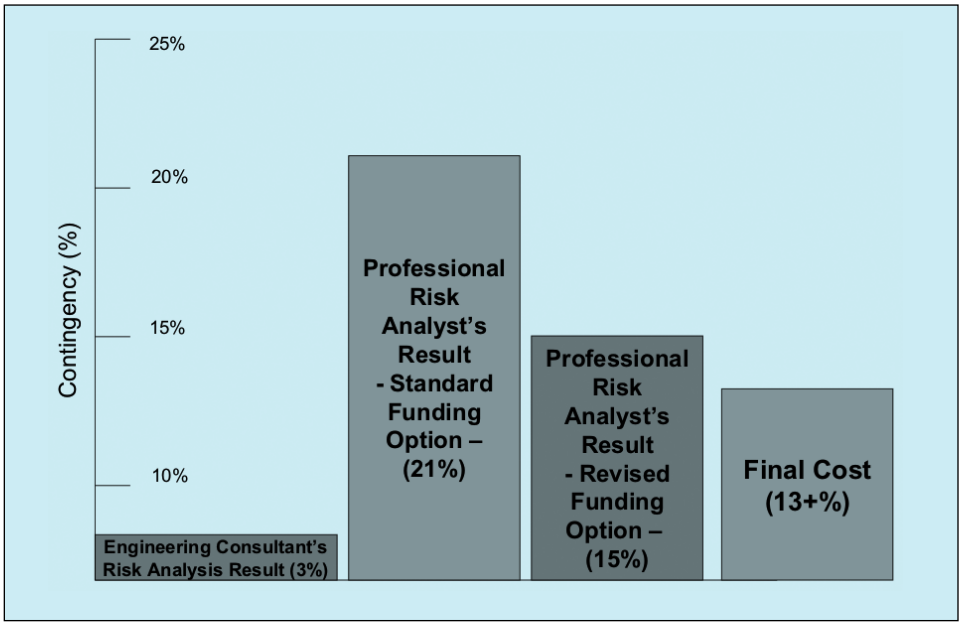

Figure 2 — Predicted Contingency (P90) Requirement

The "Expert" Executive and the Risky Analyst

A major contractor performed a risk analysis on a large-scale, multi-year energy project at the request of the owner (Fear). The analysis forecasted a total project cost of $1.9 billion at P80 ("at P80" means there is an 80 percent probability of not overrunning the associated value - $1.9 billion in this case).

After nearly one year into the project, things were not progressing according to the contractor's risk analysis. An uncertainty benchmark was conducted against the results of the initial risk analysis. (An uncertainty benchmark measures the amount of uncertainty uncovered by a risk analysis to determine whether or not its results are, or were, likely reliable. The benchmark is expressed as minimum total cost variability. In essence, the uncertainty benchmark is a risk analysis of a risk analysis.) The contractor's analysis failed the uncertainty benchmark (see figure 1).

The uncertainty benchmark indicated that the cost uncertainty derived in the contractor's risk analysis was understated by at least $495 million. Although the original risk analysis contained a number of errors, the most damaging was its inclusion of too many cost elements in a range estimating analysis (Simplification). This large number of elements resulted in a significant understatement of project cost uncertainty (i.e., risk and opportunity).

A subsequent analysis was immediately conducted by a third-party risk analyst and the results indicated that the project's cost at completion (still several years out) would be over $3 billion at P80. Upon receiving these results, an executive from the owner company demanded that the results be changed before distribution to other executives and board members (Denial and Anger).

The executive spent more than two hours explaining his own "expertise" in project risk analysis, that he had many years of experience, and that he had conducted several hundred risk analyses for energy projects (Simplification). The risk analyst refused to alter the findings.

After several years, the project was finally completed - at a total cost of slightly over $3 billion.

Steely Determination

A cost-risk analysis had been performed by an engineering consultant on a several hundred million dollar energy project at the behest of a US government agency (Fear). The analysis took several weeks to complete and included one-on-one interviews with key project personnel (Simplification). One of the project's managers became uncomfortable with the analysis since it recommended only a 3 percent contingency at P90 for the five-year long government project (Fear).

A subsequent analysis was conducted by a professional risk analyst. It showed that a 21 percent contingency was required at P90. However, the analysis further indicated that this contingency requirement could be reduced to roughly 15 percent if steel were purchased at the

beginning of the project rather than throughout the five-year construction period. This reflected the risk of steel price increases. (This follow-up analysis was conducted nearly one year prior to the significant steel price increases in the early 2000s.)

The project team was able to convince the US federal agency to front-end load some of the funding so that steel could be purchased and warehoused for the project (Acceptance). This would mitigate any potential steel price increases. The action delivered substantial savings for the project which recently completed on time and within the revised, 15 percent contingency, budget (see figure 2). A recent Government Accounting Office (GAO) report states that, of 12 mega projects it audited, this was the only one to complete on time and within budget.

Had the project been funded based on the original analysis (3 percent contingency), the project team would not have purchased steel early in the project and, even if it had, the project would still have overrun by a significant amount.

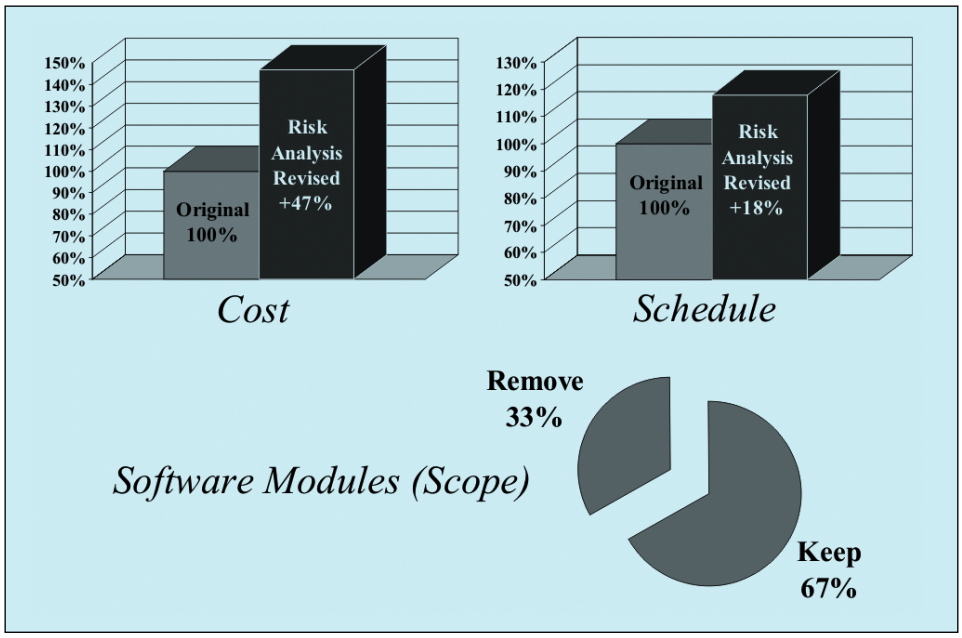

Figure 3 — Software Modules

Disinformation Technology

Information technology projects are almost entirely labor driven. As such, they can be some of the most uncertain (often riskiest) projects to undertake on a monetary basis. In one case, a risk analysis was requested on an enterprise-wide system implementation for a large manufacturing firm (Fear). Less than one week before the analysis was to begin, the third-party risk analyst was contacted by the owner to cancel the analysis. The reason: the integration firm stated that if the risk analyst was brought in to analyze the project's uncertainty, it (the integration firm) would "walk off the job" (Fear).

The owner stated that it was too bad that the amount of uncertainty would not be analyzed. The risk analyst stated that the integration firm's response, by its very nature, had already given some indication of the magnitude of risk: it was apparently high enough that the integration firm could not afford to have it surface. Eventually, the project overran by tens of millions of dollars. The owner company went into Chapter 11 not long thereafter.

In another case involving a different company, a risk analysis was conducted on an enterprise-wide system implementation due to the perceived high level of risk (Fear). In this case, the company was the second largest in its industry. The analysis concluded that, to avoid corporate-wide chaos with disastrous consequences, the cost budget should be increased by 47 percent, the schedule should be lengthened by 18 percent, and the scope (number of software modules to be installed) should be reduced by 33 percent at P80 (see figure 3).

The company followed the recommendations resulting from the risk analysis and completed the project very near its projections (Acceptance). The company subsequently received an award from the enterprise-wide software firm for having achieved the most successful implementation in that industry.

Remarkable—Compared to its original and grossly inadequate plan, one that did not include a risk analysis, the project experienced a cost overrun, a schedule overrun, and a scope reduction and yet was recognized as "best" in its industry. If nothing else, this clearly demonstrates how disastrous the outcome would have been without the interventional risk analysis.

Such outcomes are common in enterprise-wide system implementation, a territory where uncertainty runs rampant.

Taking Your Lump Sums

A risk analysis was conducted on the rebuild of a portion of a manufacturing facility (Fear). The analysis indicated that nearly 25 percent contingency was required at P80. An executive for the owner decided that the project was less risky than indicated by the analysis and was convinced that the total cost could be reduced substantially through lump sum, rather than time and materials, contracting (Denial and Simplification).

The executive took charge of the project and executed the required lump sum contracts.

The project eventually completed - significantly in excess of the lump sum contracts. The reason: several of the site condition risks which were identified by the risk analysis materialized during execution of the project. Since these conditions were outside the scope of many of the lump sum contracts, it became the responsibility of the owner to reimburse the contractors. Since most of the project was under lump sum contracts, the owner could not take advantage of those areas that underran their estimates and which could have, under the original plan, been used to offset some of the cost overruns in site condition problems.

The Shell Game

A large manufacturing company requested that a risk analysis be conducted on one of its large projects (Fear). This firm made heavy use of its own craft labor (i.e., its own plant employees). During the data gathering session, the project manager became irate and stated that none of his projects had ever overrun and that this one would not do so either (Anger). Later, during the data gathering session, a key piece of information surfaced: the project

manager had been keeping project costs under control by paying craft labor employees out of other accounts if the proper accounts would have shown an overspent status. Needless to say, that practice did keep project budgets in line but the cost overruns were still impacting the company's bottom line - in different areas of the business.

Road to Success

A large engineering contractor wanted to break into the heavy and highway business - an area in which it had very little experience at the time. A risk analysis was conducted in preparation for bidding on building a new highway. The analysis showed that the largest uncertainty in the project was the estimated borrow cost - the cost to move one cubic yard of dirt one mile. The engineering firm placed its bid based on the risk analysis results (Acceptance) but was underbid by a company that was considered "expert" in heavy and highway work.

Less than two years into the project, the "expert" company ran into a major cost problem, much of it caused by the higher than expected borrow cost. The "dirt" problem was so significant that an article was later published in an industry journal regarding the project. Dirt quality was the major topic of the article.

Eventually, the company that knew little about heavy and highway projects, but knew enough to conduct a reliable risk analysis, joined a consortium that took over the project and brought it to successful conclusion.

Blowing (Up) the Budget

A risk analysis was conducted covering the research, development and manufacturing (including per-unit pricing) for a new weapon system for the US military (Fear). The analysis showed that 19 percent contingency was required at P80. This was in comparison to the weapons developer's own analysis which indicated only 11 percent was required. The developer assessed the variabilities of nearly one hundred cost items (Simplification).

The developer became agitated regarding the third-party results and told the risk analyst that it knew its business but the risk analyst did not (Anger). Two years later, the risk analyst received a call from the US military to conduct an analysis of a multi-country weapon system development. The military told the analyst the reason for the call: the first weapon system completed with 20 percent contingency and the government wanted another reliable risk analysis conducted (Acceptance) on the new system (see figure 4).

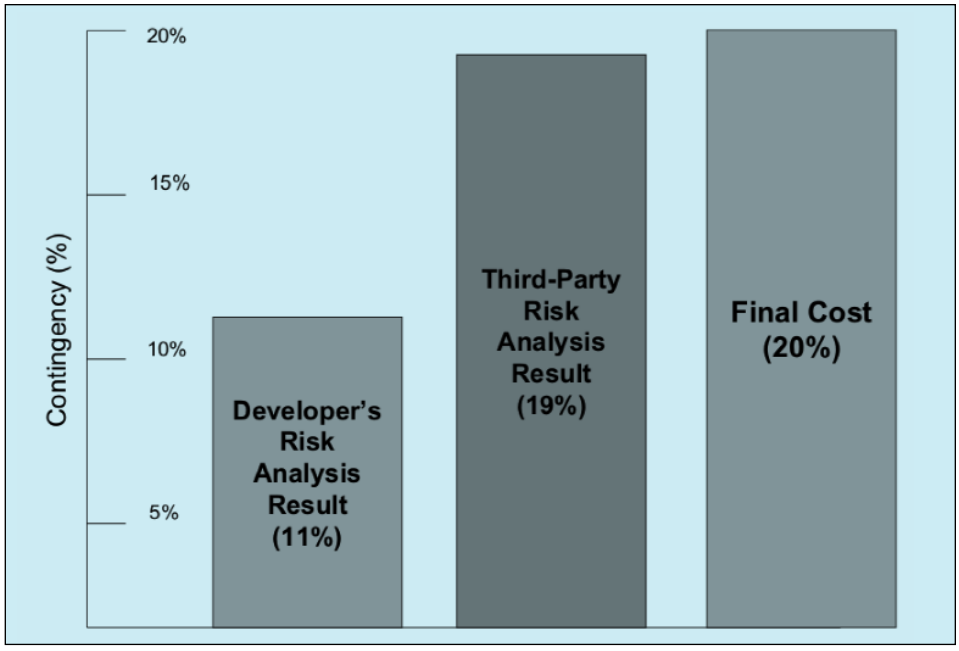

Figure 4 — Predicted Contingency (P80) Requirement

Clueless is Best

An analysis was conducted for a new, large manufacturing plant (Fear). In attendance were members of the owner's project team, engineering firm representatives, and an executive with the primary equipment supplier. Apparently, the owner had previous experience with the equipment supplier and had received equipment that was not fully assembled to the owner's specifications on previous projects.

During the facilitation session, the owner's team stated there was a risk that equipment would not be assembled as expected and that assembly would increase cost and schedule after the shipment arrived. The equipment executive stated that the shipment had already been loaded and released on a train the day prior and that the equipment was already assembled to specifications. The owner's team still had doubts and the risk analyst instructed that those doubts must be included to ensure a comprehensive risk analysis. The equipment executive became irate and, after expressing his "expert" opinion of the facilitation process, slammed the door of the construction trailer just hard enough to almost break the window when he left (Anger).

Less than two days later, the train arrived at the construction site - with equipment assembly required!

Contractor in a Box

A risk analysis was conducted on a new service facility (Fear). The results of the analysis failed the uncertainty benchmark (i.e., the benchmark indicated that the project team failed to identify levels of risk and/or opportunity expected for that type and size of project, at that stage of development). The benchmark failure was reported to the contractor and owner at which time the contractor remained adamant that the project would be well under control and that the contractor had better than average operational practices (Simplification). Several months later, virtually all bids for equipment and materials were submitted measurably over the original estimate.

In this case, as in many others, the contractor was functioning in "sales" mode - concerned that his or her admission of higher risk might jeopardize this or future business with the owner. Under most circumstances, failing the uncertainty benchmark should precipitate a follow-up risk analysis to identify the missing risks and/or opportunities.

A "Rich" History

An analysis for upgrading a large paper production facility indicated that 17 percent contingency was required at P80 (Fear). Although several prior analyses by the same risk analyst had proven reliable, this particular analysis was deemed in error by the capital project execution consultant who stated that the risk analysis provided an amount of contingency in excess of what should be required based on historical data for similar projects (Denial).

The owner decided to ignore the risk analysis results and rely on the projection provided by the historical data (Denial). The project completed at a final cost slightly in excess of the equivalent of 19 percent contingency.

Historical data is useful as a springboard for discussion regarding cost and schedule variability. However, this particular project had been estimated at a level somewhat lower than others - likely because the project team was instructed to help keep costs down on all projects during tight budgetary times. The risk analysis had successfully identified that bias. Unfortunately, reliance on historical data and industry experience could not.

Trust (Acceptance) in a risk analysis process or practice requires first that the process be proven reliable. Barring changes in scope, if a risk analysis prediction and the actual outcome differ widely, then there is likely a flaw in the risk analysis process or its execution. Post-project or post-plan excuses like, "We didn't think there was much chance of that happening," or, "We didn't think that issue was very important," indicate a failure of the data gathering process to reliably surface the true risks and opportunities.

A successful risk management program requires commitment on the part of the analysts and the decision makers. This commitment must begin with a reliable risk analysis methodology.

First, analysts must ensure that their chosen methods and technologies are devoid of (or at least help preclude) technical errors: assessing too many decision elements, applying incorrect probability distributions, assuming all elements in an analysis must or should be independent, etc. Paradoxically, analysis of too many cost items, for example, and the development of overly-complex analysis models will likely cause flawed results by understating the total uncertainty. Flawed analysis can fall shockingly short of actual results and trust will be difficult, if not impossible, to gain.

Second, special attention must be paid to obtaining the correct data for the analysis. One-on-one interviews, questionnaires, and other methods of data gathering have historically produced invalid analysis results. Although these methods are in common use, the only proven technique for surfacing key (sometimes hidden) risks and opportunities is to implement a group interrogation approach. The amount and quality of information that flows within a group environment is critical and cannot be easily captured by other means. In many cases, this approach has exposed major scope clarification issues that would have remained hidden until they were encountered in the field and at increased cost and/or schedule impact to the owners.

Once the technical aspects of risk analysis have been addressed (technologies and data gathering method), the risk management professional must ensure that information is communicated in terms that are readily accepted by decision makers.

Managers are rarely statisticians nor should they be required to become so. Like the ongoing reliability of analysis results (i.e., a track record of success), the ability to communicate effectively is essential to the eventual acceptance of the risk management program by those needing it most - the decision makers. This acceptance can be gained only if the risk management professional is ready and able to support decision makers as they traverse the risk management mindset challenges they will face.

Given a reliable process, however, managers and other decision makers must come to grips with the analysis results - regardless of how favorable or unfavorable they may be. Decision makers who use risk analysis merely to determine contingency requirements (or other necessary adjustments to any budget) will never capitalize on the real power of a sound risk analysis process - the insight and direction it provides to favorably impact the future. Those who finally reach Acceptance, will find they have a powerful tool to improve their organizations' (and their own) bottom lines.

All of this reduces to one simple question for decision makers and risk analysts alike: "Can you handle the truth?" ◆

REFERENCE

1. Risk Management Committee. **AACE International's Risk Management Dictionary**. **Cost Engineering**, Vol. 37, No. 10, (October 1995): 20-25

ABOUT THE AUTHORS

Kevin M. Curran is president of Decision Sciences Corporation. He has more than 25 years risk analysis experience having successfully analyzed more than 1,000 projects and business decisions. Kevin is co-developer of Bubble Management® and Value-Based Risk Management®. Kevin co-chairs AACE International's Risk Management Certification Task Force and can be reached by email at: kcurran@uncertain.com.

Michael W. Curran is founder and chairman of Decision Sciences Corporation and an AACE International Fellow. Michael has more than 40 years experience in the field of risk analysis and is the developer of Range Estimating and co-developer of Bubble Management® and Value-Based Risk Management® processes. Michael chairs AACE International's Decision & Risk Management Committee and can be reached by email at mcurran@uncertain.com.

CyberSection Now at AACE International Website

After nine years in Yahoo groups, CyberSection is coming home http://www.aacei.org/membership/regions/cyber/

CyberSection is a web-based section for the at-large or un-assigned members, or others, who do not have access to existing sections.

Our goal is to provide as many of the standard section services as possible—networking, presentations, mutual support, and information sharing.

Participation by members in AACE International Sections provides members one of the best connections to the true association experience. Local sections bring together like-minded professionals, offer numerous opportunities for networking and it allows younger members to find mentors in their chosen profession, and all benefit. ◆