

# Achieving Effective Risk Management by Overcoming Some Common Pitfalls

by Edmund H. Conrow

Risk management can assist managers in meeting cost, performance, and schedule requirements on their projects, yet its effectiveness is generally diminished because of inadequate processes and implementation considerations. These include:

- A weak and unstructured risk management process
- Tools and techniques that may not be well matched to the project
- An inordinate focus on risk analysis, the results of which are often relatively inaccurate and contain an unknown level of uncertainty
- Insufficient emphasis on the technical (performance) dimension of risk management
- Insufficient emphasis on organizational and behavioral issues

Each of the above items can contribute to risk management's failure. Let's consider each in turn.

## WEAK AND UNSTRUCTURED RISK MANAGEMENT PROCESS

A good risk management process includes planning, identification, analysis, handling, and monitoring

— and in that order.<sup>1</sup> Failure to include all five steps will contribute to ineffective risk management, yet it is common to find risk management processes that do not include formal planning and/or monitoring steps. For example, by not including formal risk planning, how do you know:

- What risk categories to expect (e.g., software resources, hardware/software integration)?
- What ground rules and assumptions to use for identifying, analyzing, and handling risks (e.g., planned beginning of hardware/software integration)?
- What documentation is desirable or necessary?
- What organizational roles and responsibilities exist for performing risk management?

Simply writing a risk management plan is often not enough. The risk management plan is the output of the risk planning process, it is not the risk planning process itself!

<sup>1</sup>It does not matter what you call the risk management process steps, but it is very important that the appropriate functions be performed and suitable inputs and outputs exist for each step.

To handle a risk, we have four possible options: assumption, avoidance, control, or transfer. Unfortunately, it is common to find the risk handling process step focused solely, or almost solely, on the control option (often called mitigation), rather than selecting by a trade analysis the best of the four options. By defaulting to the control option, the user forgoes what may be a better option. If you select the control option, it should be because it is the most desirable risk handling option, not the one blindly chosen. (This focus on the control option of risk handling is somewhat akin to a typical focus on risk analysis versus other process steps, as discussed below.)

Other risk management process distortions are also common, including situations where functions associated with one step are incorrectly performed as part of another step: for example, risk handling performed as part of risk identification, portions of risk analysis included in risk handling, risk planning performed after risk monitoring, and so on. What often results in such cases is an inefficient application of resources. For instance, when strategies for dealing with risks are developed

before the magnitude of the risks is estimated or before risks are prioritized, the wrong risks may have finite resources applied to them and higher-priority risks may not be effectively handled. These issues commonly contribute to ineffective risk management and increase the likelihood that key risk issues will remain undetected until much later in the project when they surface as problems, or that known risk issues will be inefficiently managed, thus wasting scarce project resources.

### RISK MANAGEMENT TOOLS AND TECHNIQUES

There is often an overreliance on tools and techniques at the expense of the risk management process structure (e.g., process steps and their order), inputs and outputs for each process step, and organizational and behavioral implementation considerations. The best tools and techniques are of little value if one or more of the process steps are missing and/or out of order or if the process is poorly implemented. The first risk management priority should be to have a suitable process with well-defined functions for each step, well-defined roles and responsibilities for implementing risk management, and a suitable environment for performing risk management.

A common abuse on a number of projects is the use of inappropriate tools and techniques or the poor application of such tools and techniques. Either case can lead to ineffective risk management. For example, checklists, taxonomies,

or templates can be helpful in identifying risks, but they should ideally be applied to similar projects at the same work breakdown structure level that they were derived from, and they should never be considered “all inclusive.” By applying a checklist developed at a very low level of software integration (e.g., the computer software unit) to a potential risk issue at a much higher level of software integration (e.g., the computer software configuration item) or vice versa, you may fail to capture some aspects of software/software integration. Similarly, if the checklist was derived from financial management projects, it will likely not be complete for real-time software that has critical timing constraints and is highly sensitive as to the target computer. Checklists should only be considered a starting point for risk identification, not the sole, all-encompassing resource.

Another technique that is commonly abused is Monte Carlo simulations for quantitative risk analysis. While the results can in some cases be very helpful to project management, proponents often oversell this technique. Output quality is strongly related to a host of factors, including:

- The model structure selected (Are the terms additive? Multiplicative?)
- The accuracy of the underlying model logic (Are sub-totals properly summed?)
- The type and number of probability distributions

representing each random variable

- The method used to estimate or measure the critical values defining each probability distribution (e.g., mean and standard deviation for a normal distribution)
- The uncertainty associated with each critical value

It is not uncommon for practitioners to gloss over or simply not understand several of these factors, yet they report results to three or more decimal places when substantial uncertainty often exists in the first decimal place!

Return on investment (ROI) is another risk management tool and technique that is sometimes abused. ROI will vary on a case-by-case basis and should be estimated in units that are appropriate to the issue (e.g., dollars for cost, time for schedule) — don’t just default to dollars. In some cases, ROI can be determined, but this is often not practical or even possible because of a lack of comprehensive, accurate data. In other cases, ROI is almost meaningless and its application would be foolish, since an ROI < 1.0 may be warranted and necessary if it eliminates a major risk that would terminate or otherwise adversely affect a project.

### EXCESSIVE FOCUS ON RISK ANALYSIS

A major yet common risk management limitation is that risk analysis is given priority in terms of resources and management

attention, to the detriment of other process steps and suitable process implementation. This is often the result of analysts, and sometimes organizations, that are in love with their favorite tools and have very narrowly focused desires and objectives. If you cannot properly specify likely risk categories, adequately identify candidate risks, develop and implement suitable risk handling strategies, or properly monitor risk handling progress, then the best risk analysis methodology will lead to ineffective risk management. In addition, there is generally little forethought as to how much risk analysis is enough — enough is enough when you have diminishing returns from a benefit-to-resource perspective, including decreasing the morale of project personnel.

Another issue is that risk analysis results often are relatively inaccurate and contain an unknown level of uncertainty, yet those performing the analysis typically do not state or even understand these limitations. We see this problem when analysts perform mathematical operations on results obtained from ordinal “probability” and consequence of occurrence scales, which are used to quantify the level of risk. (Simple “probability” scales for technology maturity and cost consequence are given in Tables 1 [1] and 2 [2], respectively.<sup>2</sup>) Here, the “probability” scale is only an indicator of probability and does not represent true probability. The nature of the

<sup>2</sup>Please note that these scales are examples only — do not use them on your project!

Table 1 — Example Ordinal Technology “Probability” Maturity Scale

Definition	Scale Level
Basic principles observed	E
Concept design analyzed for performance	D
Breadboard or brassboard <sup>3</sup> validation in relevant environment	C
Prototype passes performance tests	B
Item deployed and operational	A

<sup>3</sup>A breadboard is an item that is, in general, functionally the same as the eventual item to be fielded, but it will often not have the same form and fit. A brassboard is an item that is, in general, functionally the same as the eventual item to be fielded, and it may have the same form and fit.

Table 2 — Example Schedule Consequence of Occurrence Scale

Definition	Scale Level
Can't achieve key team or major project milestone	E
Major slip in key milestone or critical path impacted	D
Minor slip in key milestone, not able to meet need date	C
Additional resources required, able to meet need date	B
Minimal or no impact	A

scale is that less mature items have a higher score, indicating a higher level of probability that an issue will occur, while more mature items have a lower score, denoting a lower likelihood that an issue will occur. For consequence of occurrence scales, the nature of the scale is that larger potential (adverse) impacts have a higher score, while lower potential (adverse) impacts have a lower score.

While a number of methods exist to convert probability and

consequence of occurrence scores into risk levels, a simple three-level (low, medium, and high) risk mapping matrix as shown in Figure 1 is sufficient for many projects. Risks falling within a given level can then be prioritized by the risk management board (RMB) or its equivalent. It is generally unwise to develop numerical schemes to further separate the resulting risk scores, since the scores are almost always ordinal and/or an unknown degree of uncertainty exists in the results. (Although a Monte Carlo

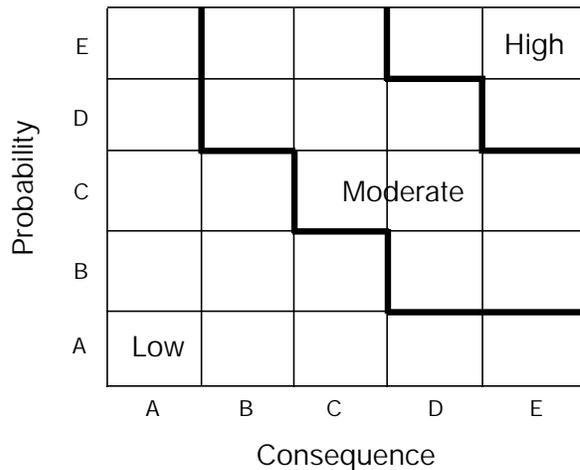


Figure 1 — Example risk mapping matrix.

simulation will directly yield cardinal risk estimates, an unknown degree of uncertainty almost always exists in these results as well.)

The example just presented does not violate any mathematical or probabilistic principles other than assuming that the technology scale values are probabilities, when in reality they are only indicators of probability (hence marked as “probability”). Note that a symmetric risk mapping matrix was chosen; when an asymmetric one is used, there is often no rationale or concrete underlying data as to why it is used or how the boundaries have been estimated. (Here, a symmetric matrix refers to the fact that the upper triangle of the matrix is the same as the lower triangle. For example, a line drawn from the origin to the upper right-hand corner of the matrix reveals that what are above and below the line are identical. Generally, specific data to support accurate asymmetric boundaries does not exist.)

As used on many projects, the underlying “probability” and consequence scales have values that are only rank ordered (ordinal), with true coefficient values that are unknown, yet the values are treated as if they are cardinal and derived from known, certain coefficients. This is why I have used letter scale coefficients (where  $E > D > C > B > A$ ) in Tables 1 and 2 to preclude people from attempting to perform mathematical operations on the results. While this may appear to be an academic issue, it can translate into very large errors both in terms of the level of resulting risks and their order (e.g., “top 10” risks that do not belong and an incorrect ordering of the risks).

A simple, irrefutable illustration of this problem is given in Table 3, where a five-level ordinal scale is constructed around US coins. Here, the ordinal (uncalibrated) scale values (1 through 5) are normalized to the upper level (5) and compared to the actual coefficient values corresponding to the cardinal monetary value

normalized to a half dollar (calibrated). The resulting error, and it truly is error, is on average almost 300%! (Other examples can readily be developed that have much larger errors.) In this example there is zero uncertainty, while in the real world there is often uncertainty in how to score coefficients, and this uncertainty is rarely if ever analyzed or even recorded. In summary, this simple currency illustration demonstrates that unless you have accurate, certain knowledge of the true scale coefficients, you should *never* attempt to perform mathematical operations on results derived from ordinal scales. Large errors can and often do occur, and such practices are almost always severely flawed regardless of how many times they have previously been used.

As mentioned above, the RMB, chaired by the project manager, should prioritize risks. The RMB should also establish the threshold of risk acceptability. If this is not done, risks will be treated in an ad hoc manner, and some issues that should have been resolved will come back later in the project as problems. This is not to say that the procedure is inflexible, but it should be structured and suitably documented, an accurate disclosure of risk analysis results should be made, and known sources of uncertainty should be disclosed. What spin upper management puts on the results is up to them. However, when the desired answer drives the results, then “being optimistic” turns into lying and invalidates the risk analysis.

Table 3 — Percent Error Between Uncalibrated and Calibrated Scale Values for Some US Coins

Item	Raw Scale Level	Raw Scale Value Normalized to Upper Level	Calibrated Scale Value Normalized to Upper Level	Percent Error, $((\text{Raw}-\text{Cal})/\text{Cal}) * 100$
Half Dollar (\$0.50)	5	1.00	1.00	0
Quarter (\$0.25)	4	0.80	0.50	+60
Dime (\$0.10)	3	0.60	0.20	+200
Nickel (\$0.05)	2	0.40	0.10	+300
Penny (\$0.01)	1	0.20	0.02	+900
<b>Average Error (%)</b>	N/A	N/A	N/A	<b>+292</b>
<b>Standard Deviation of Error (%)</b>	N/A	N/A	N/A	<b>360</b>

- (1) Raw Scale Level: Ordinal scale level for a five-level scale.
- (2) Normalized Raw Scale Value = Raw scale level divided by 5.
- (3) Calibrated Scale Value: Currency scale value normalized to a half dollar.

### INSUFFICIENT EMPHASIS ON THE TECHNICAL (PERFORMANCE) DIMENSION

While risk management has been formally applied for a number of years on a variety of projects, there is often insufficient attention paid to technical risk. This is in part related to risk management processes being developed and applied by organizations with limited if any technical focus, a situation that, again, can lead to substantial risks being missed until they surface as problems late in the project.<sup>4</sup> In such cases, it is not appropriate to merely state that technical risk is only found on, say, aerospace projects. The fundamental trades that exist on many projects are between cost, performance, and schedule, and ignoring the performance

<sup>4</sup>For example, the Project Management Institute's (PMI®) *A Guide to the Project Management Body of Knowledge* (PMI, 2000) contains no mention of technical issues or technical performance being a potential project management driver.

dimension does not mean that it is absent. (The performance dimension clearly exists for software-intensive projects as features and functions, integration complexity, etc.) Even projects that use commercial items are not immune to performance issues — many obvious common commercial components ranging from microprocessors to communications systems are priced primarily based upon performance parameters. While cost and schedule are often directly addressed in IT projects, performance may not be explicitly evaluated. Yet it is the interrelationship between the three variables that typically defines the feasibility of candidate designs and a host of other issues.

A simple but common relationship between cost and performance is given in Figure 2. Here the first derivative of cost with respect to performance is positive, but more importantly, so is the second derivative. It is this changing

relationship between cost and performance as you near the vertical part of the curve that is most troublesome from a risk point of view. This is often because the last couple of percentage points of performance available at any given point in time (e.g.,  $s = t_0$ ) correspond to a large increase in cost, which increases at an increasing rate. This holds true for a surprisingly wide variety of unrelated items, ranging from the salary of professional baseball players versus batting average to

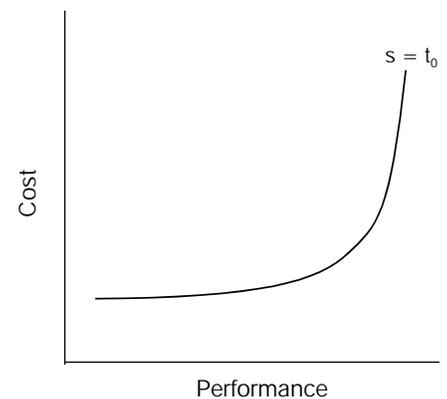


Figure 2 — Typical cost versus performance relationship.

the price of microprocessors versus clock rate, and so on [1]. It is the inability to correctly estimate the cost versus performance relationship (and other analogous relationships) that contributes to risk on many projects — and this is all the more ominous when the project is in the development phase and started with insufficient budget and schedule for the required or desired level of performance.

### INSUFFICIENT EMPHASIS ON ORGANIZATIONAL AND BEHAVIORAL ISSUES

A key impediment to effective risk management is insufficient emphasis on the organizational and behavioral issues surrounding risk management implementation. Even if an acceptable process exists, the organizational roles and responsibilities may conflict, be undefined, or even go unaddressed, and there may be no consideration of behavioral matters. Not surprisingly, documentation associated with risk management processes often contains little or no information on organizational and behavioral issues.<sup>5</sup>

<sup>5</sup>For example, the PMI's *A Guide to the Project Management Body of Knowledge* (PMI, 2000), pp. 127-146, contains no mention of the organizational and behavioral issues involved in implementing risk management. While there is no single "best" approach, some organizational and behavioral considerations for implementing risk management apply across a wide variety of projects.

For risk management to be effective, it must be implemented in both a "top-down" and "bottom-up" manner within the project. The project manager, as well as other management personnel, must be involved in both using risk management principles in decisionmaking and supporting and encouraging others on the project to perform risk management. This doesn't mean that the project manager should be the project risk manager (except perhaps on very small projects), but that his or her active participation in risk management activities and use of risk management principles in decisionmaking are essential. Without such support, other project personnel get the message that risk management is not important enough for the project manager to participate in. This can kill any attempts to create a culture that embraces risk management. In addition, upper management participation involves far more than just not "shooting the messenger." While it's important to avoid this pervasive problem, it is not enough to create a positive model for performing effective risk management.

In order to be effective, risk management must also be undertaken in a "bottom-up" manner by working-level personnel. Here, the goal is for working-level personnel to assimilate risk management principles into their daily job functions. Finally, on any project, all personnel should be expected, encouraged, and given the capability to identify candidate risk

Many proponents of risk management have little or no "real-world" experience and pontificate on things about which they have no real understanding.

issues — before they become problems later in the project.

A key reason why risk management may be on its way to being overexposed, overhyped, and oversold is that many proponents of risk management, typically those outside the project and even outside the organization, have little or no "real-world" experience and pontificate on things about which they have no real understanding. The vast majority of risk management trainers and teachers have either never had long-term responsibility on an actual program or have a knowledge base that is far below the state of the art. Yet these are the very same people that are overselling risk management.

One approach medium to large organizations can use to avoid such problems is to train a cadre of risk managers through a mentoring program. Here, a mentor is someone with substantial real-world risk management experience who assists risk managers with limited to mid-level experience on more than one project at a time. The mentor is then rotated off to another set of projects after working with the risk managers for a period of time (e.g., six months). Seasoned risk managers, including those that

have been mentored, can then be selected as mentors and help train other risk managers on the same or other projects. Within a few years, the organization can propagate a competent cadre of risk managers that can make major, long-term contributions to enabling effective risk management within the organization.

### CLOSING THOUGHTS

Risk management can greatly aid decisionmakers if it is structured and implemented correctly. The five deficiencies explored in this article are relatively common across a wide variety of programs and often limit the effectiveness of risk management. Process-related issues are often the easiest to identify and tackle, yet without addressing the organizational and behavioral issues that exist, effective risk management will generally be elusive. Trainers, teachers, and organizations that oversell risk management typically focus on a limited set of process-related attributes (e.g., tools and techniques) and have little or no experience in making the complete risk management process work on actual programs. In addition, because “cookbook” approaches do not address the difficult subject of expert tailoring to a particular project, the end result may actually be decreased risk management effectiveness versus what previously existed.

One evidence of the decline of project risk management as a credible discipline is the all too

frequent errors that exist in published papers and presentations, including those in refereed journals. It is not uncommon to find substantial errors related to the five topics discussed in this article in many published articles and presentations. Even worse, assertions are frequently made without any substantiating evidence. The typical presentation of hypothesis, outline of experiment, collection of data, analysis of data, and conclusions often jumps straight to assertions without any supporting ground rules and assumptions, data, analysis of data, etc., nor any disclosure on the authors’ part that such information even exists. While such behavior is clearly unacceptable in scientific and engineering publications, it is all too common in the project management publications involving risk management. The degree of risk management hype appears to have risen dramatically in the last few years, and this often leads organizations to form unrealistic expectations that cannot be achieved. If this trend continues, the outcome may be that risk management as a process will begin to fall out of favor instead of those individuals responsible for overhyping and overselling it being held accountable.

### REFERENCES

1. Conrow, Edmund H. *Effective Risk Management: Some Keys to Success*. American Institute of Aeronautics and Astronautics, 2000.

2. US Department of Defense. *Risk Management Guide for DoD Acquisition*, 4th edition. Defense Acquisition University and Defense Systems Management College, February 2001. (This excellent guide is available free of charge from: [www.dsmc.dsm.mil/pubs/gdbks/risk\\_management.htm](http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm).)

*Edmund H. Conrow is a management and technical consultant located in Redondo Beach, California. Dr. Conrow has over 25 years of experience in the application of project management and technical skills to moderate- to high-complexity programs. He has successfully served a broad range of clients, including industry, federally funded research centers, national laboratories, and government agencies. His practice is focused on risk management; management strategy; cost, performance, schedule, and risk trades; engineering design analysis; and technology assessment.*

*Dr. Conrow is widely published in national journals and conference proceedings, and his work has won awards at national conferences. He is a Certified Management Consultant (IMC), a Certified Professional Consultant to Management (NBCC), and a Project Management Professional (PMI®). Dr. Conrow is an associate fellow of AIAA and a senior member of the IEEE. Dr. Conrow is the author of the book *Effective Risk Management: Some Keys to Success* (American Institute of Aeronautics and Astronautics, 2000). He holds a B.S.N.E. and M.S. in nuclear engineering, M.Phil. in policy analysis, Ph.D. in general engineering, and Ph.D. in policy analysis.*

*Dr. Conrow can be reached at P.O. Box 1125, Redondo Beach, CA 90278, USA. Tel: +1 310 374 7975; E-mail: [info@risk-services.com](mailto:info@risk-services.com); Web site: [www.risk-services.com](http://www.risk-services.com).*

# Is Risk Management Going the Way of Disco?

## Opportunity

Risk management will build on its current popularity to become the most important management discipline of the next 20 years.

## Risk

Risk management will become the first management fad of the millennium — overhyped, oversold, and overblown.

## Opening Statement

Bob Charette

2

## Defining Risk: A Debate

David T. Hulett and David Hillson  
versus Ronald J. Kohl

4

## Making It Up as We Go: The Perils of Ad Hoc Risk Management

Carl Pritchard

11

## Achieving Effective Risk Management by Overcoming Some Common Pitfalls

Edmund H. Conrow

16

## Safety, Risk, and Danger: A New Dynamic Perspective

Darren Dalcher

23

## Risk Management: Here to Stay

Carole Edrich

28

## Risk Management for Software and Systems Projects: Utterly Doomed

Tim Lister

31

## A Personal Postscript: Is There a Future for Risk Management?

Bob Charette

33

# Cutter IT Journal

## Topic Index

- February 2002 Is Risk Management Going the Way of Disco?
- January 2002 The Great Methodologies Debate: Part II
- December 2001 The Great Methodologies Debate: Part I
- November 2001 BI and CRM: Critical Success Factors for Achieving Customer Intimacy
- October 2001 The Future of SPI
- September 2001 Testing E-Business Applications
- August 2001 Enterprise Application Integration
- July 2001 Web Engineering: An Adult's Guide to Developing Internet-Based Applications
- June 2001 The War for IT Talent
- May 2001 Implementing an E-Business Strategy
- April 2001 Multicultural and International Project Management
- March 2001 Developing Wireless Distributed Applications
- February 2001 Security



### Robert N. Charette, Guest Editor

Robert N. Charette is a Fellow with Cutter Consortium and the Director of its Enterprise Risk Management Practice. With more than 25 years' experience in a wide variety of international technology and management positions, he is recognized as an international authority and pioneer in information systems, technology, and telecommunications risk management. Dr. Charette is the president of the ITABHI Corporation, a business and technology risk management company. He serves as a senior risk advisor to Global 100 CEOs, CFOs, and program and project managers, as well as to senior government officials worldwide on the effectiveness, impacts, rewards, and risks of their information and telecommunications systems and other high technology programs and policies. He also acts as chief risk consultant to financial organizations and companies when investments, mergers, or takeovers are considered. Dr. Charette can be reached at [rcharette@cutter.com](mailto:rcharette@cutter.com).

## Upcoming

### Issue Themes

The Technology Myth in Knowledge Management and Business Intelligence

Legacy Architecture Migration

Web Services

Security

Design for Globalization

Open Source

Testing

XP and Culture Change in an Organization

Mobile Wireless

Preventing IT Burnout

B2B Collaboration

### Events

Extreme Programming with Kent Beck

28 April 2002, 9:00-4:00

University Park Hotel@MIT  
Cambridge, MA 02139, USA

Register now at: [www.cutter.com/workshops/extreme.html](http://www.cutter.com/workshops/extreme.html)

Summit 2002

"Business Technology in Uncertain Times"

29 April-1 May 2002

University Park Hotel@MIT  
Cambridge, MA 02139, USA

[www.cutter.com/summit/](http://www.cutter.com/summit/)