



By Pen Stout, PMP

IT project managers could learn a lot from 17th century European merchants — both have experience with uncertain, *dangerous* ventures that promise great rewards. Over 350 years ago the merchants, with some help from a monastery of nuns outside Paris, founded the modern theories of risk management. Their revelation:

“Fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event.”¹

To the merchants this meant they could calculate when their fleets would reach port and what returns they could expect. This allowed the merchants to maximize their odds over the long run to make dependable profits. As a result they could fund increasingly risky — but potentially profitable enterprises. This in part contributed to the growth of modern Western economies.

In the 21st century, IT risk management could translate to: backing up critical data, a secure power supply, documenting procedures and delegating authority when absent from the office. In short, we take precautions to secure our essential systems against the unexpected. In this the third article in our series on IT project management we will explore a practical approach to risk management using a common IT experience for an example: the design and implementation of an IT help desk.

A Practical Risk Management Process

Though risk management can involve complex statistics, the heart of the process is common sense: 1) Identify potential threats to the project cost, time and quality goals; 2) Assess each threat as the Parisian nuns suggested: determine both the gravity of the event and its probability of occurrence; 3) Create a proportionally justified plan of action for each threat. In other words, if there is a 1/10 chance of a \$1,000 loss you might spend as much as \$100 to eliminate the possibility of the threat; 4) Respond to actual problems as they occur. Rigorous risk planning will not make all the problems go away, but you will have fewer and you will be better prepared to handle them. Now let's use our IT help desk project to illustrate this process.

Step One: Identify Threats

It makes sense that once we know about a potential problem we can plan for it, but how can we know what problems we will encounter? Andrew, our IT help desk project manager, uses a common approach: he assembles a cross-functional group of project

stakeholders and asks them point-blank, *“What threats do you see to our cost, schedule and quality goals?”* In other words — they brainstorm. Andrew practices two important principles of risk identification:

- ✓ Involve a diverse group of stakeholders because both their perspectives and their tolerance for risk will differ.
- ✓ Encourage them to be pessimistic about the project and to generate as many potential problems as possible.

Other tips for risk identification are: 1) Use a common format for describing risks that distinguishes the event from the impact. Here's a good format: Event causing impact. Andrew followed the format in this risk statement: “Database server infected with virus causing staff to field help calls without access to customer data”; 2) Brainstorm first — use open-ended, concept-expanding, “blinders-off” techniques to encourage divergent thinking and catch the risks that are not obvious; 3) Check results with more convergent methods. Once the open-ended brainstorming is complete, it is good practice to check results against lists of historical risks, particularly those that apply to your specific industry, organization and program. Some project managers find it helpful to create profiles of typical risks they are likely to encounter on different types of projects. Cast a very wide net during this initial stage. The problems that hurt the most are often the ones we didn't identify early due to ignorance, denial, myopic vision or lack of discipline.

At the end of this step you will have a long list of possible problems. Now it's time to separate the wheat from the chaff. Go through the list setting aside the low-probability, low-impact threats. Place these in a tickler file. Things change on projects so you will want to review these threats in the future to confirm they remain low-probability and low-impact.

Step Two: Assess Each Threat

After setting aside the smaller threats you will still have a large number to manage, but you won't have the time and effort available to monitor all of them. How will you decide where to spend your limited time and money?

Andrew sorts the remaining threats into categories matching his functional teams: hardware, software, test, human resources, etc. Gathering the leads of each team together he asks them to analyze each threat in their respective subject areas. *“I'd like you to assign a dollar impact to each threat and an estimated probability of it actually occurring,”* he tells his leads. *“If we have experienced similar problems in the past, use our experience to improve your analysis.”* To encourage accuracy, but discourage them from getting caught up in analysis, he continues, *“It will be very helpful if you can put actual numbers into the impact and probability estimates if the numbers can be supported and it doesn't cost too much to figure them out. But don't ignore the threats that would be too hard or costly to quantify. I'd like you to give them a subjective or qualitative estimate based on the Stout- Weidner Matrix.”* (Shown on the next page.)

Andrew has his leads collect the information required to calculate the “Expected Value.” Expected Value is the product of the impact multiplied by the probability of occurrence. Here is an example: Kim identified one risk this way, *“If we have too many employees ill at one time, it causes poor response times for our users because we simply can't answer the telephones fast enough. Sometimes*

Stout - Weidner Probability Impact Matrix²

Level	Likelihood	Probability
5	Near certainty	>90%
4	Highly Likely	~60% - 90%
3	Likely	~40% - 60%
2	Unlikely	~10% - 40%
1	Remote	<10%

Probability	1	2	3	4	5
5	L	M	H	H	H
4	L	M	M	H	H
3	L	M	M	M	H
2	L	L	L	M	M
1	L	L	L	L	M

Level	Technical/Scope	Schedule	Cost ³	Impact
5	Unacceptable	Can't achieve major milestone	> 10%	Unacceptable
4	Acceptable - no remaining margin	Slip in critical path or major milestone	7 - 10%	Major Impact
3	Acceptable - significant reduction in margin	Not able to meet deadlines; float consumed	5 - 7%	Moderate Impact
2	Acceptable - minor reduction in margin	Can meet dates if additional resources are available	< 5%	Some Impact
1	Little or no impact			

callers hang-up and we never hear from them again. I'm sure this is costing us." Andrew agrees that this is a project threat and asks Kim to calculate an Expected Value. Kim reports, "I've discovered that we lose about \$1,000 a day in long-term customer business due to hang-ups whenever we don't have the right staffing levels answering the phones. This usually occurs due to a combination of poor scheduling and illness. It has occurred, on average, about 10 percent of the time." Andrew says, "We can multiply the daily impact (\$1,000) by the probability (10 percent) and calculate an Expected Value of \$100 per day. The help desk will be open 365 days a year so our annual Expected Value for this threat is \$100*365 or \$36,500 a year. That is a significant risk we better manage effectively."

Andrew will use the Expected Value of each threat to focus his limited risk management resources where they will do the most good. Andrew also recognized that the analysis of impact and probability can best be performed by the subject matter experts so he delegated these tasks to his leads. This will help the team speed through the analysis step. Andrew followed these risk management techniques: 1) Categorize the threats and delegate assessment to subject matter experts; 2) Assess cost of impact and probability of occurrence; 3) Base analysis on past history when possible; 4) Develop quantitative numbers where it is cost effective.

Additional tips for the assessment step include: 1) Accurate estimating takes time and good data; 2) Balance the need for accuracy with the cost of collecting information; 3) Estimating is better than ignoring a true threat; 4) Different stakeholders have different tolerance levels for risk. Take this into account when determining which risks to actively manage and where to draw the line. Keep in mind that active risk management requires time, effort and resources. These are usually limited so you must select which threats to manage. The size of the Expected Value is very useful for prioritizing and filtering.

Step Three: Response Planning

At this point Andrew's sponsor asks to see the list of threats. She looks it over with a frown. "Andrew, this is still a very long list. I really don't know if this project is a good idea if so much can go

wrong. What do you suggest I recommend to the Chief Financial Officer?" Andrew responds, "We are just getting to the big payoff in good risk management. The next step is to plan how the project team can reduce the surprises and control the uncertainty. Can you give me until next week to pull together a complete recommendation?" His sponsor agrees, but advises that the CFO will want to know if the project still makes good business sense. "Numbers and dollars will persuade me to take this further. And I need them by COB [Close of Business] Wednesday," she says.

When team members gather in the project room they find a list on the whiteboard: "Avoid, Transfer, Mitigate, Fallback Plan and Monitor, Accept and Reserves." Andrew opens the meeting, "We need to plan how we can reduce our current risk exposure. This is a list of ways (Figure 1) regarding how we might respond to each threat. I'd like each of you to look at your risks, starting with those having the highest Expected Value, and determine which response makes the most sense. I will want to know: 1) What actions you propose? 2) How much they will cost to implement? 3) How much it will reduce the total Expected Value of your threats list? Once you are done we will get back together to decide which actions we can afford as a team and what to do about the remaining risk exposure."

Response planning process

✓Determine the best response for each managed risk. For each approach consider the initial Expected Value of the threat, the cost of the response and the predicted reduction in Expected Value. Select the most cost-effective response. For example: Kim proposes to reduce the probability of poor phone response due to poor scheduling by hiring a consultant to teach the team how to use the software already on their computers. Training costs about \$6,000, but it reduces (mitigates) the Expected Value of this threat from \$36,500 to \$24,000 due to improved planning and coordination. She is also investigating wellness programs that might reduce staff sick days and the resulting poor response rates.

✓Add all resulting actions to the project's WBS (Work Breakdown Structure), budget and schedule to assure they are managed like any other project task.

Avoid

Avoid the threat entirely by changing the way the project is performed or by de-scoping the portion of the project that contains the risk element. Be careful with this approach. Eliminating the risky scope might disappoint a critical stakeholder or degrade the business reason for performing the project.

Transfer

Transfer involves moving the responsibility for a threat to another party usually by payment of a fee (outsourcing to a skilled expert) or a premium (insurance).

Mitigate

Take positive actions to reduce either the impact of a threat or the probability of it occurring. Mitigation usually requires positive action and has a cost. These actions should be reflected in your WBS as new work packages and controlled like any other part of your normal project.

Fallback Plan and Monitor

Sometimes it is too costly to mitigate or transfer a threat but we still want to keep an eye on it. In this case design a fallback plan to put in effect if the event actually becomes a problem. Then implement a method of actively monitoring for occurrence of the problem. Remember that not all problems announce themselves with a loud knock on the door. Some emerge slowly. These will require well-designed trigger events so monitoring can identify the emerging problem at the earliest moment. It is often easier to fix a problem early in its development before it gains momentum.

Accept

After trying to avoid, transfer or mitigate the threats to your projects, you will be left with residual risks, threats you can't reduce further. The final strategy is called acceptance. We will discuss the residual risks and decide together with our sponsor if we can accept them as a potential cost of doing the project.

Reserves

There are two types of reserves: Contingency and Management. Contingency reserves are funds held back for identified threats — the residual risks we have decided to accept (known). Management reserves are those funds held back for unidentified threats (unknown).

Figure 1. Andrew's handout for response planning

✓ Review the total residual Expected Value. Determine a contingency reserve sufficient to cover this remaining risk exposure. Negotiate it with your sponsor.

Additional Tips: 1) Reserves should be held separate from the allocated performance budget. They are released as work packages only when a threat becomes an actual problem and requires corrective action; 2) Reserves usually cover financial impacts. Some scheduling approaches, such as Critical Chain Project Management, also attempt to provide extra time to cover the uncertainty in estimating task durations and project schedules. This time reserve is often called a buffer. In some organizations it is standard practice to sandbag or artificially inflate estimates and quotes to assure sufficient resources are available to cover the unexpected. Unfortunately such *fudge* usually gets *eaten* as work expands to fill the time or budget available. This is a poor management practice.

At the next meeting the team reviewed everyone's proposed threat responses. In a couple of cases, two responses to different threats conflicted with each other so the team worked out mutually supporting responses. The required actions were added to the baseline project plan. The next day Andrew brought his risk plan (Figure 2) to a meeting with his sponsor. She was pleased to see that the team had developed a proactive approach for many of the project threats and agreed to help negotiate a project contingency reserve with the CFO. *"He'll be very happy to see that you have identified and taken positive action to reduce the possible surprises in this project. He doesn't like project surprises because they reduce his ability to deliver on his promises to the CEO and Board of Directors. I'm sure he will agree to a good reserve if we can assure him it will not be eroded by poor performance. Oh, and have Kim give me a call. I think we can help with the financial justification for that wellness program if it really works."*

Step Four: Continuous Risk Management

One of Andrew's team members remarks, *"That risk management*

exercise was interesting, but now it's good that our focus is back on the real tasks of getting this help desk up and running." Andrew responds, *"I'm glad you are concentrating on the project tasks, but I want to point out that the risk process doesn't go away just because we have performed an initial risk exercise. We will need to stay current with the risk effort just in case things change."* Andrew knows that all risks have not been identified or eliminated. He will follow these principles during the rest of this project:

- Make risk identification a regular part of project team activities.
- Ask for new risks at every project status meeting.
- Update the status of risks. If the probability or impact changes, maybe the response needs to change. If a response works and the risk event passes with no problem, note the success and retire the risk from the log.
- At key project points, such as when a phase ends or at significant changes in scope or personnel, perform another formal risk assessment.

Some Cultural Challenges

Some managers appear to be practicing denial as a form of risk management when they demand a "can do" attitude and accuse those focusing on threats of being pessimistic whiners. They may not understand that risk management is a well-formed, proactive process that delivers value by focusing limited resources on the reduction of surprise. When this is the case the politically savvy project manager will engage in tactful education emphasizing the benefits of improved control.

Implementation of the process will require discipline at several levels including the team and executive levels. The team must realize that risk requires constant attention coupled with routine effort to limit exposure. Executives will have to gauge the long-term benefits of active risk management and balance it against the short-term need to fund risk management activities.

Project leaders managing enterprises like aircraft carriers and

Future event	Poor phone response due to scheduling and illness	Database server down due to virus	Insufficient incoming telephone capacity during crisis
Probability	10%	5%	7%
Impact	\$1,000 / day	\$750 / day	\$25,000
Expected value	\$100 / day (\$100 * 365 = \$36,500 / year)	\$37.50 / day (\$37.50 * 365 = \$13,688 / year)	\$1,750
Total expected value of identified risks			<u>\$51,938</u>
Response	Mitigate risk by training in scheduling software	Avoid risk by using a system not connected to the Internet and enforcing strict controls on all upgrades	Transfer risk by paying phone company to guarantee available bandwidth
Response cost	\$6,000	\$5,000	\$1,000
Probability - after response	6.6%	0.0%	2%
Impact - after response	\$3,650	\$0	\$25,000
Expected Value - after response	\$24,000	\$0	\$500
Total response cost			\$12,000
Total Expected Value			<u>\$24,500</u>
Reduction in uncertainty			<u>\$27,438</u>

Figure 2. Andrew's risk management breakdown - partial

nuclear power plants, which require very high reliability, have learned that uncertainty is the enemy of reliability. They successfully battle it by creating a culture of mindfulness at all levels. They use both formal and informal methods to constantly scan for potential problems while fully empowering an active threat response by all team members. Move your project team into this culture and deliver better performance with fewer surprises to your sponsor and customers.

Summary

Risk management is a systematic process that reduces the potential for unexpected project outcomes and improves the project manager's ability to meet or exceed the expectations of key stakeholders. It adds value to the project effort by increasing the probability that sponsors and customers will receive what they expect, when they expect it, for a price they expect to pay. Stripped to its essence, risk management is a set of methods for answering a few, common sense questions: What could go wrong? How wrong could it get and what can we do about it?

The ideas are simple. Like most things, the payoff is not in the knowing, but in the routine doing. Discipline and practical, routine application are key. Once you and your teams internalize the process and use it on a day-to-day basis you will find a sustainable improvement in project performance and stakeholder satisfaction. These simple ideas really work wonders because they get the odds working for you — rather than against you — and that's a truly sweet spot to be in.

References

1. Hacking, Ian. *The Emergence of Probability: A Philosophical Study of Early Ideas about Probability, Induction, and Statistical Inference.*

Cambridge University Press, 1975. Chap. 8, p. 77. Hacking describes the activity of nuns working in association with Blaise Pascal at the Port-Royal monastery in 1662.

2. Derived from Eric Verzuh, Dr. Harold Kerzner and DoD.

3. These are considered acceptable variances in stable, mature, competitive industries with high selective pressure for accurate estimation. An overrun of 10 percent for a new publicly-funded stadium would be considered terrible, an aerospace firm may or may not consider a 10 percent overrun a problem depending on the type of program, while a software product developer would consider a 10 percent overrun to be the best performance he has ever seen.

Sources:

A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Project Management Institute, 2000.

Risk Management Guide for DoD Acquisition. Defense Systems Management College Press, 2000.

Kerzner, Harold. *Project Management/Project Management Workbook.* Van Nostrand Reinhold, 1995.

Leach, Lawrence P. *Critical Chain Project Management.* Artech House, 2000.

Verzuh, Eric. *The Portable MBA in Project Management.* John Wiley & Sons, 2003. Chap. 6.

Weick, Karl and Sutcliffe, Kathleen. *Managing the Unexpected.* Jossey Bass Wiley, 2001.

Pen Stout is a project management consultant and trainer. He coaches firms as they implement project management and he conducts project leader training for the Versatile Company. Contact him via www.versatilecompany.com. □