

Risky Business

Wayne Turk



A good risk management process ... should be used to continuously assess what can go wrong in the project, determine which of the risks are most important, identify the potential effects or outcomes, and implement strategies to deal with them.

Skating on thin ice, sky diving without a reserve chute, flashing a full wallet in a bad neighborhood, unprotected sex, rooting for Dallas from the middle of the Redskins' cheering section—all of these have one thing in common: there are significant risks involved. It is the same with managing a project. But guess what, that's why they invented risk management.

Risk management is a discipline for living with the possibility that future events may cause adverse effects. A

good risk management process to identify and mitigate the bad things that can happen is a necessity for program managers. It should be used to continuously assess what can go wrong in the project, determine which of the risks are most important, identify the potential effects or outcomes, and implement strategies to deal with them. Looking at any of the risky activities above, there are ways—some simple and some more complex—to avoid or mitigate the risks involved. PMs need to do the same with project risks.

According to Al Ware, senior risk manager at Space and Naval Warfare Systems Command, Charleston, S.C., "The process of managing risks within DoD is an accepted concept and has been a requirement for almost two decades. It is not a passing fad. It has been clearly documented as a key element of the top best business practices, especially among Fortune 500 businesses. Every few years the wording of the DoD directives requiring the management of risks has been made stronger and stronger until it is definitively mandatory."

The Risk Management Program

The Project Management Institute uses the systems approach in the *Guide to the PMBOK* as a recommendation for implementing a risk management program. The approach covers six major areas:

- Risk management planning
- Risk identification
- Risk assessment
- Risk quantification
- Risk response planning
- Risk monitoring and control.

Turk is a consultant with Suss Consulting. He is a retired Air Force lieutenant colonel and defense contractor. He has supported information technology projects, policy development, and strategic planning projects for DoD, other federal agencies, and non-profit organizations. He is a frequent contributor to Defense AT&L.

Let's take a brief look at these areas.

The Plan

Everything in DoD starts with a plan. The risk management plan presents the strategy and ground rules, defines the stakeholders, sets the objectives of the program, defines the process and organizational structure, and presents roles and responsibilities. It may also contain the template(s) for the documentation associated with the program. It is also helpful to create (or copy from others, if possible) the defined risk areas. Some common areas of risk are technical, financial, project management, and environmental. The plan should also present requirements for prioritizing and for closing the risks. There is probably a good example of a successful risk management plan somewhere in your organization. Find it and tailor it for your project. Many organizations have a central risk management group—a good idea, as this concentrates experience, knowledge, and a single process in one area. They can help you with your specific project needs and provide processes and good advice.

The Identification

Identification of all of your risks is extremely important. The initial identification can come from anywhere or anyone but usually comes from someone on the project team. The form used to submit risks may be based on whatever format is desired or standard in the organization, although a Microsoft® Word document is commonly used for submission, and a spreadsheet is usually used for tracking. Initially, the PM (or risk manager) will go out to the team and others to request risk inputs. Don't worry if there are a large number. That's actually a good sign—it means people are taking it seriously. As time passes, new risks will be identified and added to the list while some old risks will drop off. Sometimes it requires a nudge to get people to identify and submit risks. They worry that risks reflect badly on them individually or on the project.

The Assessment

Risk assessment means evaluating the risk. The assessment begins with an analysis, whose depth will vary with the project. Assessment is tied closely with risk quantification, which is based on the results of the analysis. A combination of the probability and impact (which together define the severity) will determine whether the risk can essentially be ignored or will require close monitoring. The simplest type of quantification is a risk matrix with axes being *probability* and *impact*. Using general rating categories (high, medium, and low) along each axis will give results that could range from low/low (essentially ignore) to high/high (you'd better watch this one closely or you may be out of a job). The higher the severity, the more monitoring or action it needs and the higher priority it should be given. Also, the higher the priority, the more detailed the analysis that is required.

The Quantification

There are many detailed and complex methods of quantifying or ranking risks. One good analysis of these can be found in *Preparing for the Project Management Professional (PMP) Certification Exam*, 2nd Edition, by Michael W. Newell. There are a number of other good sources.

The Response

The result of the assessment also serves as the basis for determining the response strategy. Sometimes—as they used to say in the math books—the strategy “should be intuitively obvious to the most casual observer” (a hated phrase by students because frequently it wasn't very obvious). There are several different approaches using up to 16 strategy elements/choices, but these four are considered the basic strategies for most users:

- **Elimination/Avoidance.** Ridding your project of the risk completely is cost-prohibitive or very difficult, if not impossible. And if you could eliminate or avoid it, it wouldn't be a risk any more and could be closed.
- **Transfer.** Shift the risk to someone else or into an area where consequences are more tolerable. Sometimes this can be done by contracting out the source of the risk, especially by using a fixed price contract. However, after transferring the risk, you may be dependent on someone else and may not have insight into what is happening. The final result could be a bad surprise.
- **Acceptance/Monitoring.** For risks with a low ranking or priority, this is an acceptable method. It is also a possibility when the cost of mitigation is too high to be acceptable. Then the risk should be monitored until the severity (probability and impact) becomes unacceptable.
- **Reduction/Mitigation.** Determine a strategy that will reduce the severity of the risk to an acceptable level. The strategy might be a different (lower-risk) technology, more testing, a change in personnel, or any of a hundred other mitigation strategies.

Einstein reputedly said “It is not possible to solve a problem using the same thinking that created it.” David Hilson, in *Innovative Risk Management*, says risk management requires fresh thinking, namely in the development of effective risk responses. Hilson also says that “just identifying risks is not enough, and if appropriate action is not taken, then risk exposure will remain unchanged. However deciding what is ‘appropriate’ for each risk demands a degree of innovation, being prepared to consider and implement actions which were previously not thought necessary.” In other words, you may have to be creative to mitigate your risks. Creativity is one of the things that PMs are paid for.

The Risk Management Organization

Since risks can affect any or all areas of a program, one accepted idea is to have the risk management control at the highest level of the organization practicable. This can

15 Bad Reasons for Not Using Risk Management

- We have no risks.
- Identifying and making risks public will kill the program.
- We deal with problems as they arise.
- My customer/boss/whoever doesn't want to hear that he/she is the source of risk.
- You can't predict what will happen a year from now.
- No one on the staff knows how to do risk management.
- We plan to start implementing risk management next year.
- There is nothing in it for me.
- Our job is to develop megawidgets, not fill out bureaucratic forms and go to stupid meetings.
- If I gave a realistic risk assessment, no one would listen.
- That method/process/tool/software/hardware is not a risk. X said so.
- This project is too small to do risk management.
- We can't identify risks based on government (or industry) metrics because our project/process is different.
- Things are going smoothly. We're on schedule and under budget.
- We don't have time.

Based on excerpts from The Little Book of Bad Excuses, Software Program Managers Network, June 1998.

save resources or provide economies of scale for solutions. While the higher-level the control, the wider the reach, there is also less direct contact or oversight at the working level. Therefore, it might be better to have a central RM function but have the function also at the project level. Representatives from all levels should be involved to ensure that multiple perspectives are incorporated, more risks are identified, and better control strategies are developed.

The following are some roles and responsibilities in the RM program for a typical organization. Names and specific responsibilities may vary, but this provides an outline of an RM organization within a program. In some cases, positions and responsibilities can be combined.

- **Program Manager**—has overall responsibility for the program and projects, including RM.
- **Risk Management Manager/Director**—responsible for the risk management program; usually chairs the Risk Management Committee/Board.
- **Risk Management Committee or Board**—drawing members are from all levels and parts of the organization, provides overall guidance to risk management activities. This includes periodic reviews of all (or at least

the most significant) risks, validation of risk information, assignment/approval of risk ownership, reviews of risk response strategies and status, and approval for adding or closing risks.

- **Risk Manager**—maintains the RMP and risk database, ensures information is up to date for the Risk Management Committee/Board, and provides administrative support to the Committee/Board, requests input/updates from risk owners.
- **Risk Owner**—PM, functional integrated project team lead, or task manager over the area containing the risk; responsible for some or all of the analysis, and developing response strategies; also responsible for monitoring the risk and providing updates to the risk data base.
- **Risk Action Managers/Team Members**—assigned by the PM or task manager and responsible for specific actions under the response strategy.

Processes

While processes will be different among organizations, there are some activities that should take place in almost every risk management program. The first of these is the risk database. This is a living document, updated periodically (read as “frequently”), and cannot be just “shelfware.” In the submission and tracking of risks, the following information is suggested as input.

- **Name**—use an individual and easily understood name for each risk.
- **Identification number**—each risk should have an individual number for easy tracking; this is usually assigned by the Board/Committee or the risk manager.
- **Description**—a write-up with enough information to adequately and accurately describe the risk (this sounds simple, but can be very difficult).
- **Date**—the date that the risk is presented to the Board/Committee or accepted as a risk.
- **Person responsible for managing**—usually assigned by the PM or risk manager and can be the person who identified the risk (although that has a tendency to cut down identified risks if people think that they will be responsible).
- **Probability of occurrence**—usually general categories like high, medium, and low, or a specific estimated probability from 0 to 1.
- **Impact**—what happens if the threat comes true? How will it impact the project? If the impact is a dollar cost, it should be estimated and revised as necessary. The impact should have a rating, either general or numerical. Many organizations use numerical values from 1 to 5, with 1 being minimal impact and 5 being maximum impact—a “showstopper.”
- **Severity**—this can also be general categories or a specific numerical value.
- **Mitigation strategies**—how the project will avoid, reduce, or mitigate the risk. This should include cost, milestones, and a timeline.

Ware says that “severity is also referred to as the risk Exposure Value. The exposure of the risk is the first indicator on the severity and is a significant tool in aiding the RM team in prioritizing risks. The exposure is automatically calculated in some risk databases (e.g., Risk Radar (available from SPMN)).”

As mentioned earlier, risks can be identified and submitted by anyone. Once submitted, they should remain in draft status until the Committee/Board approves them for entry. Once the risks are approved, it may require significant analysis work or modeling to determine the impact to cost, schedule, or performance. For these major risks, some type of a repeatable analysis or modeling process is needed.

The Committee/Board should meet periodically. The frequency might be anywhere from weekly to quarterly, depending on the number and level of the risks. For most DoD programs, monthly is probably about right. In preparation for the meeting, the owners of all risks will update the status. At the meetings, there should be a review and approval/disapproval of draft risks for inclusion in the database, the status of the highest priority risks (the “Top 20” is a good guide), and any risks that can be closed. On many projects, the risk status is also briefed during IPRs using some sort of a stoplight chart (red, yellow, green).

The risk database should be available for view by everyone in the program. A caveat here is that sometimes a risk, even a very low-level risk, can make people start worrying about their jobs. This is especially true with funding risks. However, that issue is offset by the fact that when people know about risks, they can work to resolve or lower them.

The risk manager should also hold periodic reviews with risk owners. In some cases, this is also a part of the Committee/Board meeting. However, a separate meeting is recommended so that there can be detailed discussion of the status, milestones, etc.

Closure

Closing a risk is a happy time for all. It is done when the risk is no longer a risk (duh!). The risk could have been overcome by events, resolved, or completely transferred. The last—completely transferred—can only be closed if it no longer is a risk to the project. The closed risk needs to stay in the database with all of the appropriate information and dates, but in a closed status.

According to Ware, technically speaking, a risk is also closed when it has transitioned into a problem, and the PM needs to invoke planned contingency actions. There are two schools of thought on the proper use of the contingency plan: Use the contingency plan as a backup mit-

If you don't identify, assess, and respond to risks, your project could go down the tube and take you with it.

igation plan in case the initial actions do not successfully mitigate the risk down to a more manageable level; or use the contingency plan for what the team will do when you-know-what has hit the fan.

The final process should be the completion of a lessons-learned report, or a white paper, or entry into a lessons learned database. In the report, there should be both specific lessons learned and general lessons learned that might apply to other areas. Most organizations have some kind of a standard format.

No amount of teaching and no RM tool will enable a team to successfully protect a project if that team does not have the right “cultural attitude” toward risk management. In *Project Risk Management*, Bruce T. Barkley says, “A risk management culture can be defined as the ‘prevailing standard for how risk is handled.’ An organization with a strong risk management culture has policies and procedures ... to go through disciplined risk planning, identification, assessment, and risk response project phasing. A mature organization does not treat risk management as a separate process, but rather ‘embeds’ the risk process into the whole project planning and control process.”

Risk management is one of the most important areas of project management. If you don't identify, assess, and respond to risks, your project could go down the tube and take you with it. Einstein defined insanity as “doing the same thing over and over again and expecting different results.” In other words, no lessons learned.

As the Chinese proverb says, “If we don't change direction we're likely to end up where we're headed.” And if you don't do good risk management, you are headed down the road to failure. Risk management helps identify when you are heading in a potentially wrong direction and helps you change direction so that you don't end up “where [you were] headed.”

The author welcomes comments and questions. Contact him at wayne.turk@sussconsulting.com or rwturk@aol.com.