

First Things First

The Importance of Risk Identification

Douglas J. Bragdon

You are the government program manager for a high-volume production program. Your contractor team is beginning to build components based on the hardware design that was completed in the developmental phase of your program. Schedule must be maintained. You are confident, however, because even with a tight budget, you insisted all along on a robust risk management program.

Late on a Friday afternoon, less than a week before your first article is scheduled for testing, your technical director and your risk manager burst into your office.

“We can’t get the parts to fit,” the TD says. “We’ve tried everything. We have no choice but to reopen the design.”

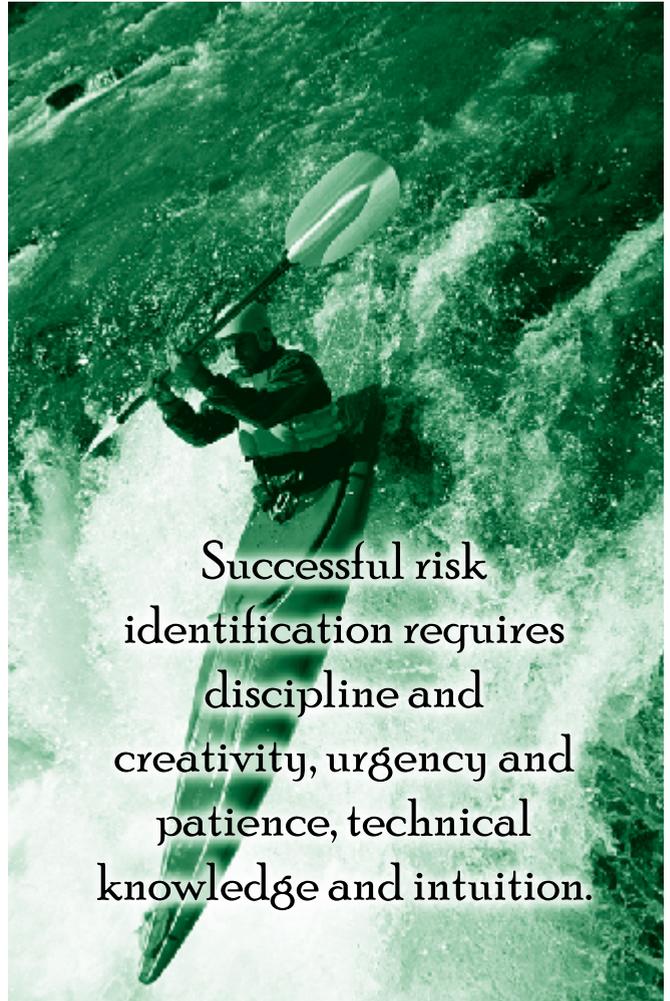
“Why didn’t we see this coming?” you ask.

“Well I thought we took care of this through our risk program,” she says. “A simulation would certainly have identified this problem. But Bob here says this risk fell off the raft six months ago.”

“We actually proposed this risk three times,” says the RM. “When we started out with our Delphi solicitation two years ago, over half of our industry experts mentioned it. But the contractor PM said that industry just didn’t understand their design and that it was not a risk. So it never got onto the contractor risk register.

“Several months later it came up at the preliminary design review. The government team insisted that the contractor conduct a formal risk analysis. The following month, the contractor briefed it as a second-tier risk being handled at the cost account level. There were too many other important risks. After a couple months, it disappeared. And no one noticed.

“Then six months ago, the risk team scrubbed the program against the manufacturing risk model, which encourages a simulation early in the program. We discussed it and people felt that if we really needed one, we would have done one earlier.”



Successful risk identification requires discipline and creativity, urgency and patience, technical knowledge and intuition.

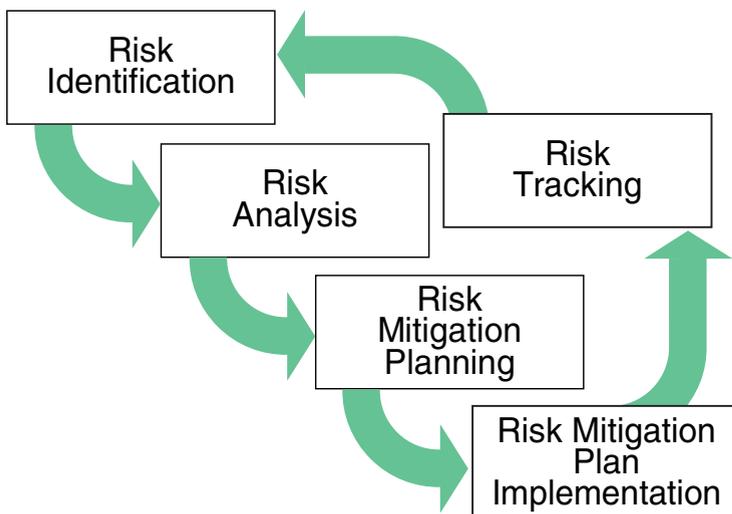
This is the day you hoped would never come—a sizeable schedule slip, cost growth, and an angry customer. You swear never again to waste money on risk management.

It Happens All the Time

The episode described above is hypothetical, but similar incidents happen all too frequently in developmental contracting. With the increased emphasis on risk management over the last 10 years or so, nearly all large developments mandate a risk program. Contractors develop finely tuned risk statements to assess their risks, guided

Bragdon spent over 20 years in engineering and project management within DoD. He now works as a senior systems engineer for McClendon Corporation supporting a compartmented DoD program

FIGURE 1. DoD Risk Management Process



by commercial risk management software packages. Each month at the program management review, they proudly display their risk matrix to justify their program-level risks. If they have enough initiative, they will attempt a quantified assessment to estimate the current cost of these risks, and they may apply that amount of resources to mitigation plans. Yet major risks go unaddressed. In the end, risk management has become something it should never be—just another engineering checklist—and has drifted far from the dynamic, creative, and predictive approach necessary for success.

Worst of all, too many times, the risk that rises up and threatens serious damage to a program is one—such as the flawed design mentioned above—that could have been identified and mitigated at minimal expense. In retrospect, you may find the killer risk buried obscurely among second tier risks, below the line for funding mitigation plans, stymied by “phantom” top-level risks that weren’t.

The growth of risk management in the Department of Defense over the last 10 years constitutes a critical improvement to acquisition. Schedule, budget, even entire programs have been saved through effective risk management processes. But there are still too many programs that needlessly suffer from predictable and manageable risks.

In order for the DoD risk management process to increase in value to programs, it needs to move out of its adolescence and become fully matured. The key to this maturity is improvement in the most important, yet most elusive part, of the process: *risk identification*.

Risk Identification—What Goes Wrong?

My thesis—that risk identification is the most important part of the process—may seem unconventional. But consider the example described above. The ultimate prob-

lem was not mitigation or resources, it was an inability of project leaders to recognize an impending risk despite numerous opportunities. A simulation would have spotted the problem, but no one realized the importance of doing that simulation.

The failure was in the risk identification portion of the process. Risk identification is the activity that determines which risks are relevant to the program. As Figure 1 shows, risk identification is iterative; it must be properly executed on a continuing basis in order for the overall risk management effort to add any value. Nevertheless, there is no surefire formula for success. Successful risk identification requires discipline and creativity, urgency and patience, technical knowledge and intuition.

In a typical high-risk, high-payoff development scenario, the risk effort normally gets off to a strong start. The technical staff are energized by the impending challenge, and the first meetings produce creative brainstorming sessions during which (often for the first time) the technical details of the effort at hand begin to be fleshed out. There may be daunting challenges, but there is also confidence that the technical expertise can meet them. And, of course, there is that risk mitigation resource pool for the really hard stuff.

Wait Up—Not so Fast

Once the first pass is complete and presented, the government PM is most likely impressed with the work and commends the team. At this point, several bad things could happen. First, the risk team might begin to think that the risk identification phase is done. We’ve identified the risks, they think. We’ve sketched out technical mitigation approaches that correspond to the gravity of each risk—now all we need to do is execute the plans.

Nothing could be more wrong. For a new development effort, the technical risks will continue to evolve well into the design phase. And it often happens that the risk team is made up of a number of strong senior- and mid-level engineers, each of whom has a history of building successful systems. Their strength may well be to execute within a clearly defined scope—to build to the spec. They may not be comfortable remaining in the frame of mind that risk management requires—one in which the rules may change dramatically at any time. Finally, it is difficult for anyone to continue to go over the same ground with a fresh and energized approach, looking for new risks. This is like asking a beat cop to take over a cold case investigation. The risk meetings may quickly become stale and perfunctory.

The situation can be made worse if the PM misuses the output of the risk identification or predetermines what the program risks should be. Consider the effect on the

team if one of the topmost identified risks is scuttled by the PM. Even if the PM's reasons are solid and he or she communicates them clearly to the team, the amount of energy put into the risk identification process will be drained. Worse yet, the risk team may begin to defer to the PM's intuitive sense of risk to the program—and when you get to that point, there is little value in continuing the process. A higher priority, informal, and unstructured process has taken precedence.

Another major obstacle to an accurate identification of risks is that meaningless phantom risks arise on the roster in front of the team. The risk roster too frequently becomes the medium for all sorts of finger pointing and maneuvering. One case is the common temptation for components of the technical program to identify dependencies on other components as their own risks. For example, when software and hardware are being developed in parallel, there's a risk if there are no hardware platforms for software engineers to use for development. But it is a program risk, not a software risk. It is of no benefit to anyone for the software team to sit in meetings discussing a lack of hardware. This risk should be accepted by the risk owners (hardware development and program management) and managed at the program level. Software can then move to assess the specific risks to software development—normally a fertile ground for risks.

In its effort to produce results for both the government customer and its shareholders, the prime contractor normally needs to evaluate risks that may stand in the way of success in reaching the goals (and profits) associated with the contract—in other words, contract risk. It's a necessary business practice, but it should not be conducted as part of a government program using government funds and resources. Contract risks should be identified and managed in a separate business process outside the terms of the contract.

Get the Most from Your Risk Program

In order to get the value you need from your risk management effort and the most for the resources you are dedicating to this activity, you—the PM—must take an active role. Some PMs participate actively as a member or leader of the risk identification effort. This is not necessary, but it is acceptable as long as the PM doesn't bring in ancillary concerns from other aspects of the program, thereby over-

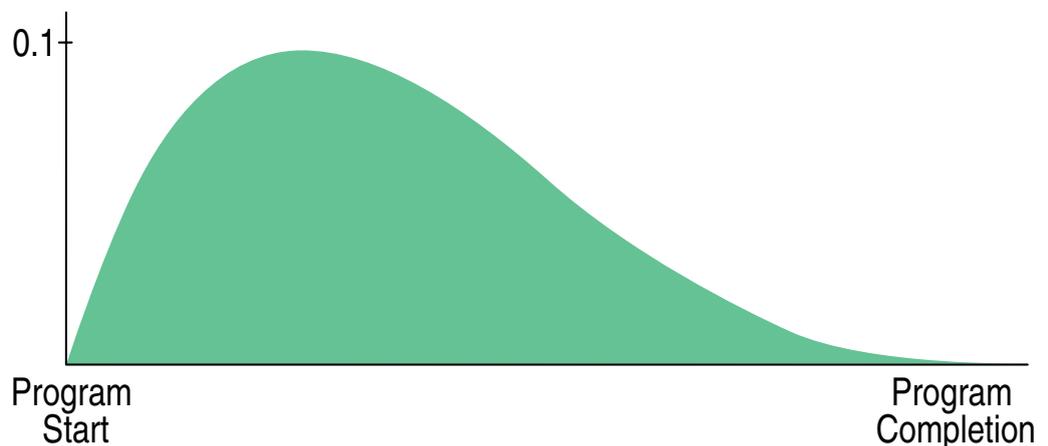
whelming the risk identification process. The brainstorming component (which nearly always includes dead-ends and tangents) must play out in a nonjudgmental, unpressurized environment.

After the customer, the PM stands to gain the most from proper risk management and must recognize the essential nature of the effort. The PM needs to be a strong, nonjudgmental listener with an open mind toward candidate risks. He or she can enable risk management by fostering a strong initial risk identification effort, by embracing the results, by measuring success, and by maintaining the validity and viability of the effort through its most useful and necessary period.

Your project's initial risk identification, if done well, will identify many of the risks that could affect your project throughout its life. For a development effort, however, it cannot be expected to identify them all. The initial risk identification must be followed up by a continuing effort to identify newly occurring risks. The beta distribution (Figure 2) illustrates that the most important time for planning and funding risk management initiatives is the first half of the project, through the design activities.

For the initial risk identification, insist on multiple strategies. The choices are well known—brainstorming, Delphi technique, models, expert opinion, and so on. Make sure the risk team uses more than one approach and makes a concerted effort to bring in outside opinions. Risk models, such as the software risk taxonomy published by Higuera and Haimes through the Software Engineering Institute at Carnegie-Mellon University, are simple tools that document the areas where similar programs from the past have encountered risk. A simple, structured approach using a model may sometimes illuminate risks that are otherwise “hidden in plain sight.” For example, applying the software development model may force the team to address the question of testing for all software units. The initial risk identification should address the en-

FIGURE 2. Distribution of Risk Expenses





Far too often, risk identification results are received with polite thanks—then left in a file.

tire scope of the project, not just the beginning. This is because the risks from the later periods may need to be managed from the outset.

Once the initial risk identification is complete, and the management strategies are in place, risk identification must continue, and PMs must take pains to sustain the effort. Painful as it may be, keep several of your most creative engineers on the effort. At least once in each phase of the program, insist that the team exercise an alternative risk identification approach. A periodic meeting of an advisory board made up of industry experts can provide a valuable balanced assessment of program risk, and the benefits to the program will far exceed the cost.

Embrace Risk Results

Risk management can't succeed unless it is properly resourced, prioritized, and empowered. This may seem to be an obvious statement, but far too often, risk identification results are received with polite thanks—then left in a file. There are as many reasons for this sort of behavior from a PM as there are causes of stress—budget, schedule, customer satisfaction, team dynamics. But this cannot be allowed to happen. A confident program manager will realize that there are many unknown unknowns on a development project and should resist the impulse to ignore inconvenient possibilities. Not all mitigation strategies can be funded, and in the end, there should be a brass-tacks reckoning regarding whether funding the risk mitigation is worth the investment. But the time for that is when all the information is in.

At the same time, the PM can strengthen his or her program with a constructively critical approach to risk identification. Have the risk team explain how they have assessed the entire scope of the effort, not just the first challenges out of the gate. Ask about those risks that you intuitively sense that don't show up. Make sure that the contractor is keeping program risk separate from contract risk (and is paying its own way for contract risk as-

sessments and mitigation strategies).

Measure Success

If quantifying risk is an inexact science, then measuring the benefits accrued through implementation of risk management strategies is even more difficult. It must be done creatively and carefully. Optimally, none of the risks identified for your program will ever occur. Still, even if the risks never occur, the costs of a well-planned mitigation strategy are

worthwhile. More telling is the documentation of program issues that never appeared on the risk roster. If a program suffers a series of technical setbacks that were not being mitigated, there may be some critical flaws in the risk identification process. A mid-program lessons-learned session may bring to light why those risks were missed—and how they might have been caught.

For risks that are being managed, the PM can build measurement criteria into the mitigation plan; just as with any money you spend, you want to understand how to measure its value.

Earned Value Management Systems are only marginally useful in measuring the performance of risk management. While being developed, risk strategies are normally level-of-effort tasks, which give no true assessment of value. However, negative cost reports and schedule variance reports are a good place to start in a holistic, retrospective assessment of risk identification: How many negative variances were caused by known risks, and how many were totally unexpected?

More Art Than Science

In practice, the execution of risk identification is often substandard. To be done well, this seemingly simple step must be more of an art than a science. Too often, the risk roster becomes loaded down with phantom risks, while real risks are underfunded or ignored. For development programs this can have drastic implications. There may be significant cultural reasons that cause a good process to fail. You, as the PM, can take steps to ensure that a strong risk identification process is in place to give your risk analysis and the rest of your risk process a fighting chance..

The author welcomes comments and questions and can be reached at doug.bragdon@mcc-corp.com.