Risky Business

Why DoD Needs a New Risk Management Paradigm

Thomas H. Miller

Department of Defense Instruction (DoDI) 5000.2—"Operation of the Defense Acquisition System"—the DoD's "Bible" for Program Management (PM), uses the word "risk" 67 times within its 80 pages but only has a minimal passing reference to "Risk Management" in the section related to service contracting, defining it as "An assessment of current and potential technical, cost, schedule, and performance risks and the plan for mitigating or retiring those risks."

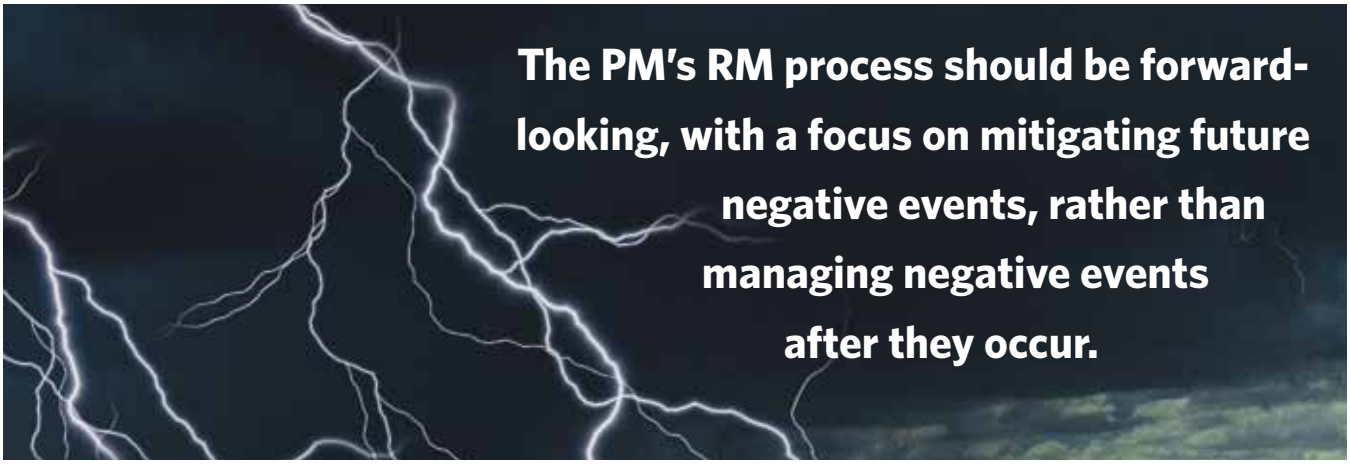
The Project Management Institute (PMI) *Guide to the Project Management Body of Knowledge* (also known as the *PMBOK*) includes a much longer chapter on Risk Management (RM). Given that risk is a significant concern in DoD program/project management, why is the process of managing risk given such short shrift in the DoDI 5000.2, particularly in comparison to the commercially focused *PMBOK*? Is the commercial PM community more concerned with RM than is the DoD community?

Miller *is the assistant program executive officer (program management) within the Program Executive Office for Land Systems (Marine Corps) and is a former Marine Corps program manager and Army contracting officer. He currently is working at the Joint Staff J-8 Capabilities and Acquisition Division on a rotational assignment.*

The answer to the second question is "No, both are (or should be) equally concerned with RM." The answer to the first question is the basis for this article. The lack of guidance on RM in the DoD acquisition "Bible" is indicative of a curious lack of focus on RM within the DoD acquisition leadership organization, in terms of repeatable processes, standardized documentation, and adequate training for personnel.

I believe this lack of focus is a proximate cause of the continuing problems DoD has had in delivering consistently successful results for its programs. Most DoD program/project managers (PMs) implement RM processes for their programs, but my experience is that these are halfhearted, "check-the-block" efforts that do not capture the true risks of the program or, even worse, that sugarcoat the actual risks. In either case, program risk is underreported to leaders and stakeholders, and unmitigated risk events quickly turn into serious issues.

Simply stated, RM is a continuously iterative process that includes several steps: identification and measurement of program risks and their root causes; identification and implementation of appropriate mitigation measures; and tracking and reporting the risks through retirement. The DoN Risk Policy states: "An effective risk management process is evidenced by early identification and analysis of risks, planning to mitigate those risks, early implementation of corrective actions, and continuous tracking and reassessment." Note the key words in this statement—"early" and "continuous"—emphasizing again that an effective RM process needs to be proactive and reassessed continuously. Due to the dynamic DoD environment—with rapidly evolving technologies, continual threat changes, and arbitrary funding cuts—PMs need to conduct (and reconduct) RM reviews regularly, to make sure new or changed risks are identified and appropriate mitigation plans are executed.



The DoD acquisition leadership needs to recognize the importance of rigorous, proactive RM, provide clearly documented guidance that requires PMs and Program Executive Officers (PEOs) to establish and implement RM processes in their programs, and ensure implementation through independent, senior-level reviews of risks at program technical and milestone events.

An Overview of Risk Management in Defense Acquisition Programs

Despite the lack of coverage in DoDI 5000.2, there actually are several good, common-sense publications and instructions available on RM in the DoD community. I will leverage two of these heavily in this article: the Defense Acquisition University (DAU) *Risk Management Guide for DoD Acquisition* (hereinafter referred to as the *DAU Risk Guide)* and the Department of Navy (DoN) Instruction titled Naval SYSCOM Risk Management Policy (hereinafter referred to as the DoN Risk Policy).

The *DAU Risk Guide* makes a clear statement of the importance of RM: "Risk management is a key element of a PM's executive decision making. DoD risk management is based on the principle that risk management must be forward-looking, structured, continuous, and informative."

Risks vs. Issues. A risk is an uncertain, possible future event that could have a negative impact on a program's outcomes and deliverables, particularly those cost, schedule, and performance requirements identified in the Acquisition Program Baseline (APB). An issue can be defined as a risk that has already occurred—i.e., a negative impact currently occurring or that has occurred in the past. The *DAU Risk Guide* points out the significant difference in managing risks vs. issues: "A common misconception, and program office practice, concerning risk management is to identify and track issues (vs. risks) and then manage the consequences (vs. the root causes). This practice tends to mask true risks, and it serves to track rather than resolve or mitigate risks." In summary, the PM's RM process should be forward-looking, with a focus on mitigating future negative events, rather than managing negative events after they occur. This difference has been compared by Paul Lohnes and Cheryl Wilson to "fire prevention" vs. "fire alarms"—a good analogy, as most would agree it is better to prevent a fire than clean up after it has occurred.

Planning the Plan: Risk Management Objectives, Process Steps, and Definitions.

There are several common, recommended steps in establishing a RM process for a program. The first step, of course, is

documenting the process in a program Risk Management Plan (RMP). The *PMBOK* explains the purpose of the RMP: "The risk management plan describes how risk management will be structured and performed on the project." In short, the RMP describes the end-to-end process for risk management on the program; helping to ensure that the process is performed thoroughly and iteratively. The *PMBOK* also states that the RMP shall include the following content: Methodology, Roles and Responsibilities, Budgeting, Timing, Risk Categories, Definition of Risk Probability and Impact, Probability and Impact Matrix, Revised Stakeholders' Tolerances, Reporting Formats, and Tracking. So the RMP needs to address the famous "Five W's": who is involved in the process; what steps are involved; the "whys" of the process (i.e., what are the objectives of the process); when is the process performed (how often); and where is the process performed (location and resources); as well as the one "H"—how will the process be performed in support of the program.

The RMP is the most important RM tool in the PM's toolbox. It establishes and documents the program RM process, identifies roles and responsibilities in the RM process, provides a common lexicon for RM communications inside and outside the PM Integrated Product Team (IPT), and ensures that risk is managed adequately and appropriately throughout the program life cycle. Publication of the RMP as early as possible in the program life cycle is the most significant step the PM can take toward program success. The RMP is intended to be a "living document" actively used, referred to, and updated regularly. As stated in the *DAU Risk Guide*: "As a program transitions through developmental and operational testing, and then to end users during sustainment, a program RMP should be structured to identify, assess, and mitigate risks that have an impact on overall program life-cycle cost, schedule, and/or performance." Since the RMP is meant to be used regularly by the PM IPT, it should be as simple as possible in content and format, and should include only the minimum essential information required to fully document the program RM process.

The Concept of Formally Accepting Residual Risk. Residual Risk is defined in the DoN Risk Policy as "the risk that remains after mitigation." Why is this concept important? In the DoN process, the PM IPT conducts two passes through the risk assessment portion of the RM process. In the first pass, the risk is assessed and classified without mitigation applied; and in the second pass the risk is reassessed and reclassified (using the same Probability/Impact Matrix) assuming the selected mitigation(s) have been effected. The result of the second pass assessment is called "Residual Risk." The benefit of this two-pass approach is that it ensures both full assessment of the risk and that the appropriate risk mitigation action is selected. Also, under the DoN process, the level of authority that can formally "accept" the risk is based on the Residual Risk rating, with higher-level risks requiring higher-level approvals, both in terms of programmatic authority (up to the Milestone Decision Authority) and technical authority (up to the commander of the Systems Command). This process ensures "top cover" for the PM, as well as increased situational awareness on program risks for the senior leaders who own the program.

Why a Proactive RM Process and Culture Matters. The essence of risk management is to actively anticipate future negative events and take immediate action to mitigate their potential effects on program results and deliverables. It can be argued that "proactivity" and "risk management" are interchangeable terms. Lohnes and Wilson state that proactivity is the highest stage in their "Risk Management Maturity Model": "Proactivity is both cost-effective and valuable in a risk management program since dealing with mitigation is considerably more efficacious than trying to 'play catch-up' after a known risk has triggered into demanding reality." Proactive RM is driven both by process and culture. A well-developed and -implemented RM process will force PM IPTs to continually assess their programs' risks. But process alone is not enough. PMs and senior leaders also need to foster a culture that incentivizes and rewards PM IPTs who conduct honest, thorough RM, and who transparently communicate those risks to all stakeholders. Dr. David Hulett states: "Commitment to risk awareness is a main action that an organization should take to make a risk management program successful. Creating the atmosphere that makes communicating about risk possible and safe to do is a key component of the risk aware culture." Culture change is by far the hardest part of implementing an effective RM process. It is driven from the top down; and requires continual effort. Senior leaders need to allow the PMs and their program IPTs the latitude to identify risks aggressively and freely report them up their chain of command, while stressing the importance of the RM process through clear policy, as well as through due diligence reviews and approvals of program risks. Such senior policy, support, and oversight currently are missing from the DoD, as evidenced by the lack of emphasis in the DoDI 5000.2, and ultimately by the continued poor DoD program performance record. As a result, PMs generally develop reactive and shallow RM processes, rather than the proactive, in-depth RM processes such technically complex programs require, and paper over serious risks in order to keep their programs moving forward.

How Do We Fix The DoD RM Process?

Hopefully, the foregoing brief, top-level discussion has been persuasive in establishing that current RM policy, processes, and overall emphasis on the topic are not sufficient for the highly complex DoD acquisition programs. Here are a few recommended steps that DoD leadership can take to improve this situation:

- Immediately acknowledge the problem and take steps to fix it. DoD acquisition leaders should publicly admit the current lack of policy and focus on proactive RM in their programs, and take positive, expeditious steps to correct this problem. The first step would be to form a senior RM

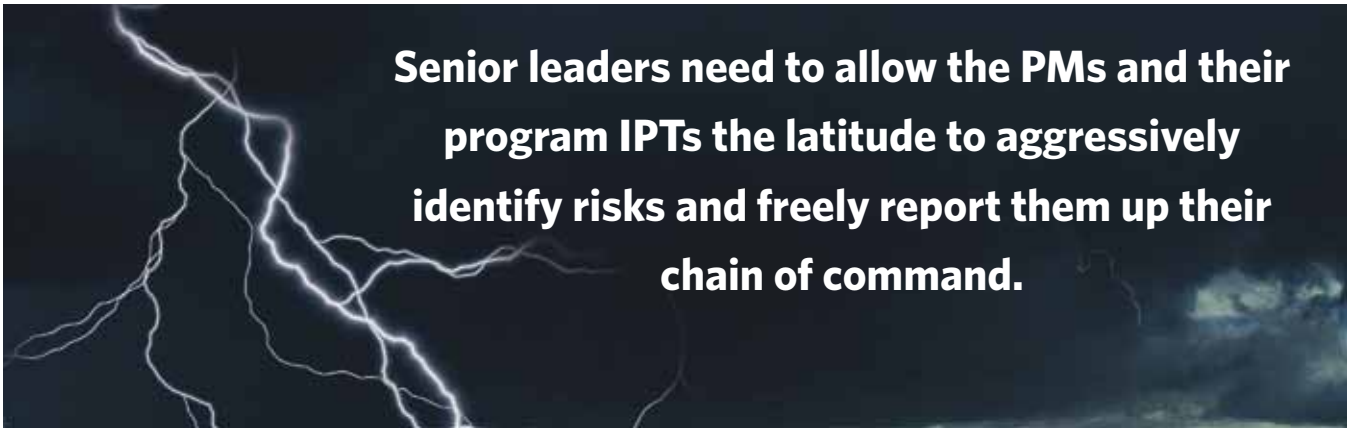
steering group within the Acquisition, Technology and Logistics (AT&L) organization, led preferably by the under secretary or, at a minimum, by a director or assistant secretary. This group would become the RM process owners. The steering group members then should form a Working IPT (WIPT), and task it with quickly developing appropriate policy, documenting a more robust, rigorous process. The new RM policy could be promulgated by AT&L directive, followed by appropriate modifications to DoDI 5000.2. The RM steering group and WIPT should continue to monitor implementation and execution of the RM process.

- Improve the rigor of acquisition training on RM. The RM steering group should concurrently task the DAU with an "end to end" review of current acquisition training content, with a focus on recommending ways to increase emphasis on RM. DAU then should conduct an expedited phase-in of the new RM content, with initial focus on PM certification training, but eventually expand to all career certification coursework.

- Service Acquisition Executives (SAEs), PEOs, and PMs should take ownership of the RM process. Leveraging the new policy of the Office of the Secretary of Defense (OSD), the individual Services should take aggressive measures to improve RM direction in their internal acquisition policy documents (for example, the Secretary of the Navy Instruction 5000.2). For major defense acquisition programs, the Service Acquisition Executives (SAEs) should form a senior-level Risk Management Board (RMB) to review and approve residual program risks and mitigation strategies. This board should be integrated into internal service program review processes and events (such as Navy Gate Reviews and Army Systems Acquisition Review Councils).

- PEOs and PMs should implement proactive, transparent RM processes in their programs. PEOs and PMs should review their current RM processes, including program RMPs, and take appropriate steps to make them more proactive and forward-looking (rather than reactive), ensure that PM IPTs actively and honestly assess and report program risks, and establish approval review processes for residual risks and associated mitigation plans. Every program—regardless of Acquisition Category (ACAT) level—should be required to have an RMP, approved by the PM and PEO or Milestone Decision Authority, and assign a risk manager. Key stakeholders should be represented on the program RMB, particularly technical warrant holders in order to ensure independent assessment of technical and safety risks.

- Leadership at all levels should continually push for a RM-focused culture. Through policy, words, and actions, leaders at all levels should encourage a positive RM culture within the DoD acquisition workforce—one that awards open and honest assessment and discussion of risks and root causes, and emphasizes proactive, action-oriented RM processes.



One Final Point—Risk Management is Not Risk Aversion

In the course of assessing the current DoD RM processes, discussing their readily apparent shortcomings, and recommending ways to implement more robust, proactive policy and processes, one should not infer that I advocate developing a risk-averse culture. Quite the opposite—I believe DoD should be more willing to take risks in order to ensure and expand the edge our warfighters enjoy. But those risks should be well understood, mitigated, and communicated before they occur. Establishing a robust, proactive RM process is absolutely essential in making this happen. The current weak, reactive DoD RM process actually results in greater risk aversion, as risks that are not identified and actively mitigated early on quickly turn into issues that bust cost, schedule, and performance metrics, leading PMs and their IPTs to be more conservative in planning and executing future programs, with negative implications for acquisition life-cycle costs and schedule durations. Programs with proactive RM programs result in more predictable results, which in turn improve the confidence of program personnel and stakeholders.

The author can be contacted at **thomas.h.miller3@usmc.mil**.