Risk Management Rollout and Installation at the NRO

Acquisition reform provides government program managers and their contractors more opportunities than ever before, but it also greatly increases risk. It is no surprise that Department of Defense (DoD) organizations face reduced resources, deplenishment of critical skills, increased congressional and public scrutiny, and a demand for streamlined operations and quality program results. The need for risk management is becoming apparent. But how? When program managers are under pressure to meet accelerated schedules and within budget, can risk management be integrated into already-burdened programs? This article shows how the National Reconnaissance Office (NRO), an organization with a dual DoD and security mission, introduced a disciplined risk management process that has provided significant cost-benefits.

DoD organizations increasingly operate as partnerships: government program managers and contractors are responsible for producing sophisticated and complex systems through integration of capabilities to deliver program results. The pressures that affect the DoD community also impact the NRO. This organization experiences the additional challenges of meeting mission requirements that integrate DoD and security missions. The organization faces a combination of new technologies, system complexity, tight schedules, and often-unstable requirements. With increased congressional oversight and public awareness, the NRO is experiencing pressure to deliver more complex and accelerated security programs than ever before.

In December 1995, the Undersecretary of Defense, Acquisition and Technology issued a memorandum, *Reducing Life Cycle Costs for New and Fielded Systems.* It acknowledged that "There are risks to be taken and risks to be avoided. When risks are taken, we will put in place appropriate risk management and contingency plans" [1]. The most recent guidance, released in May 1999, *Risk Management Guide for DoD Acquisition*, strengthens this policy. Risk management is defined as "an integral component of policy and strategy to develop and field systems responsive to user needs" [2].

NRO leadership has also directed that risk management is a critical element for program success. In fact, NRO Directive 7 of policy document *NRO Acquisition Management* emphasizes:

"Effective acquisition planning and aggressive risk management by both government and industry are essential for success. Program decisions and resource commitments must be based on consideration of executable options and plans for, and progress in, controlling risk" [3].

The *Catch-22* in today's context is that, while risk management is more necessary than ever, finding time and resources to install a sound program creates a need to prove real and lasting value. As many who have tried to install risk management in their programs know, expanded awareness of its importance, and guidance on desired results, do not necessarily translate into effective, interactive processes that provide desired results.

For the past two years, the imagery intelligence (IMINT) organization at NRO, in partnership with the Software Engineering Institute (SEI), created and installed a risk management process that became an integrated aspect of program operations. The full story of this risk management initiative is available in *Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office*, a December 1999 technical report published by SEI [4]. Three critical success factors in this program installation were:

1. Visible and committed sponsorship.
2. Culture change that supported open communication for the surfacing and mitigation of risks.
3. A disciplined, forward-looking, continuous risk management, infrastructure, and rational, well-thought-out installation process.

These three critical success factors are interlocking and mutually reinforcing. Each of these was present and engaged at NRO, as described below.

Committed, Visible Sponsorship

"Leaders do not have a choice about whether to communicate," says Edgar Schein, professor at the MIT Sloan School of Management. "Leaders send messages whether they wish to or not. People in organizations are constantly looking to their leaders for cues about what is acceptable behavior. And it is not merely public statements that people hear and believe; it is the entire range of messages sent through behaviors and their consequences, organizational mechanisms, and events that have impact" [5].

The original pilot Risk Management program was undertaken by the Command and Control Division (CCD) at IMINT. This was the first NRO program to engage in a full-scale risk management program [6].

This pilot project was not without its challenges. The initial reaction by CCD participants was a measure of skepticism coupled with clear expression of their expectations.

"We were not interested in just learning a new vocabulary," said one area manager, "if risk management did not help us get our jobs done every day, then we were not interested. Risk management needs to show value by providing cost-efficiences, better scheduling, and technological capability."

The CCD division chief, and his area manager that he charged with risk management, decided that their best opportunity to achieve results with risk management would require a unified, coherent, disciplined process that involved all division staff. Accordingly, the division held a risk clinic to create its focused process. Once the decision was made to build a risk management infrastructure and process, the CCD division chief decided it was important that he be present at all critical meetings. The division chief integrated risk management into technical assessments, program reviews, and the monthly joint government/contractor meetings to manage joint risks, the Team Risk Reviews (TRRs).

As a result, the government program managers and contractor managers created a dialogue that, over time, opened communication to a level of candor that provided technical, schedule, and cost mitigations. An example of an early suc-

cess resulted from identifying a risk in the methodology by which the program planned to manage its Operations and Maintenance (O&M) process. Up to this point the O&M activities and the development activities were separated into different organizational elements under different contracts.

Due in part to this segregation, the processes were inherently expensive and made it easy for deplenishments in functionality to occur. The risk mitigation strategy was development of the Integrated Development and Maintenance Organization (IDMO). The IDMO absorbed the maintenance functions traditionally managed by the operational site and integrated them into the development organization. The goal was to gain synergy through a single reduced staff that would manage a consolidated maintenance and development effort.

The sponsorship factor is undeniable: both government and contractor managers exhibited clear support for necessary changes to achieve constructive outcomes.

Once the pilot program had proved the value and efficacy of risk management to the satisfaction of this division and to Al Krum, the system program director, he decided to install risk management at the system level.

Recognizing the importance of focus on the entire program, he confirmed that, for risk management to be successful, "Management commitment is invaluable. Managers cannot assign risk management leadership to individual contributors; risk management will not be taken seriously without appropriate and visible leadership" [4].

As evidence of his commitment to risk management throughout his system, Krum launched the Executive System-level Risk Management Team (ESRT), that included all division chiefs, to lead the way for risk management by other divisions across the system. Next, he directed that each division would undergo training in risk management processes and procedures, to develop a common language and set of tools to use within divisions and across the system.

In addition to authorizing a rollout and installation process across the organization, Krum "walked his talk." During development of the risk management process, division chiefs continued to question the durability of sponsorship for risk management. Although Krum had clearly stated his sponsorship for risk management, there were mixed views regarding management's seriousness about the initiative. To reinforce his commitment, he used various forums to present his vision for the risk management effort and his expectations for coherent, consistent communications up the chain to management. The result was strengthened support of risk management by most division chiefs, as well as evolving practices within the divisions.

> A risk management infrastructure is essential to support the kinds of communication necessary for effective risk management.

To further clarify the seriousness of risk management at the system level, the program manager led the division chiefs to define the level of risks appropriate for system-level discussion. Accordingly, the ESRT defined its criteria for system-level risks as follows:

- Impact on program commitments.
- Risks deemed as priority due to being on the program's critical path or on any division's critical path.
- Exceeded planned schedule slack, and those that resulted in a negative margin (seriously eroded management reserve).
- Cost impact exceeds planned budget.
- Impact on program interfaces, internal or external to the program.

System risk management allowed the program, for the first time, to analyze and work together on interdependencies at the system level. Through the division risk management processes and the ESRT, a consistent system process was installed. As divisions installed their own process, they were increasingly able to communicate mission-critical risk management concerns to their contractors.

Culture Change to Support Open Communication, Risk Mitigation

The 1999 DoD *Risk Management Guide* emphasizes a risk management approach that is disciplined, forward looking, and continuous [2]. "Our goal," program director Krum said in describing IMINT's aim of risk management, "was to build a system in which people would think ahead, mitigate risks, and reduce the likelihood of system delays, depletion of management reserve, and system failures.

"To accomplish this, we knew that risk management would require a culture change to one where people would openly discuss those very areas that are most likely to be uncomfortable. We wanted to build program success on a platform where leaders and contributors *put their cards on the table*" [4].

NRO had undergone a number of studies that analyzed specific cultural barriers to effective program functioning. In particular, a study by Malcolm Baldridge in 1996 pointed to a need for NRO to move from a culture of risk avoidance to the kind of open communications that elicit widespread knowledge and information sharing [7]. Risk management, in particular, requires early and open exchange of key information to allow for timely mitigation. Several studies have shown that, in the great majority of program failures, one or more key technical project staff knew in advance there was a serious risk of failure.

The forums established at IMINT provided for this kind of discussion. Krum said, "Risk management forums at both system and divisional levels are not so much a place where you 'don't shoot the messenger' as one where 'there is no messenger to shoot because there is not a crisis yet.'" [4]

In the example cited above, the advent of an IDMO organization was not readily embraced by the O&M organization. O&M members thought that it took away some of their flexibility to utilize level-of-effort resources to address the new approach, and required a scheduling discipline that was contrary to the organization's existing business practices. In addition, the maintenance budget would be turned over to development.

Open-forum discussions established in the monthly team risk review meetings allowed identification of a potential budgetary risk in the newly configured approach. The risk was that the original O&M program might not have budgeted sufficient resources to support new archi-

tecture being delivered.

As details of the risk were developed and discussed openly between government and contractor, it turned out that there was a budget shortfall. With this early identification, the management team could provide a budget wedge and secure necessary funding to acquire key resources and meet availability requirements.

To arrive at this level of candor and critical information exchange, leaders set the tone. Contributors and others must accept accountability to support the effort. A risk management infrastructure is essential to support the kinds of communication necessary for effective risk management.

Of course, all government organization, including NRO, have grown change-weary. To foster acceptance of risk management, a building of trust in the process was necessary, so that it would not be seen as the *change process du jour.* The risk management infrastructure supported the growth of trust in the process.

Risk Management Process and Infrastructure

To leverage a lasting risk management process across a complex system, where the pressure of current crises can erode the best intentions, a sturdy yet streamlined infrastructure is essential. For new initiatives that create a culture change, building a solid, well-designed infrastructure to support the change may initially seem burdensome. However, the infrastructure, if well-planned, can become a support for ultimate efficiencies and integration across system program management. The infrastructure further supports an alert, continuous process of risk management watchful for emerging and changing risks over a program life cycle.

A key driver behind the installation process at IMINT was to support division leaders who could provide sponsorship, model risk management behaviors, and act as in-house mentors for the process over time. Another critical element was to install a smoothly functioning operational infrastructure (teams, processes, practices, and information resources) to leverage continuous risk management and improvement of the process.

The infrastructure installed at IMINT included the following:

- Conducting software risk evaluations with government and contractors for the pilot program to identify initial program risks and plan mitigation strategies.
- Establishing divisional risk management practices, which include regular forums where risks are identified, planned, tracked, and controlled—in staff meetings, program review sessions, or specified risk reviews.
- In some cases, establishing goverment/contractor integrated product and process team-type TRRs for monthly identification, planning, tracking, and control of joint risks.
- Establishing the system-level risk management team, where division chiefs and the program director or his deputy meet monthly to discuss and monitor system-level risks.
- Designing a communications architecture that provides clear guidelines to all staff members on roles and mechanisms for communicating and working risks.
- Developing consistent, system-wide risk information documents, tracking charts, and a custom-tailored risk management tool initially designed by the CCD pilot program, eventually leveraged for system-wide use.

These streamlined infrastructure elements supported the risk management process at IMINT, and in turn are increasingly supported by the expanding risk management community. The contributors at IMINT found a return on investment in risk management that ranged from such subtle changes as "awareness has increased; we no longer just look at today's problems" to major crisis-averting risk management. IMINT still bears fruit.

As a final example, a mission-critical risk identified early on during one of the original IMINT risk assessments in 1997 was a portfolio of related risks involving scheduling and specifics of system-level testing, which were key to successful program delivery. In response to this major risk, an integrated set of mitigation strategies were translated into a mitigation plan. The mitigation plan received clear guidance from the government sponsor, with collaborative input from government and contractor TRR team members. With close monitoring at the monthly TRRs and ESRT sessions, and with instantiation of several contingency actions, the program delivery was not only on time, but successful in all defined aspects.

Conclusion

While risk management program integration is almost never easy, as an IMINT contractor said, "It is important to do the hard right thing than the wrong easy thing." By applying the three key success factors outlined above—committed sponsorship, a culture moving toward more open communication, and a reliable infrastructure to support continuous risk management—IMINT achieved successful risk management results in support of mission-critical programs into the new century.◆

References

1. *Reducing Life Cycle Costs for New and Fielded Systems, Undersecretary of Defense (Acquisition and Technology) Memorandum,* December 1995.
2. *Risk Management Guide for DoD Acquisition, DoD Test, Systems Engineering and Evaluation, Defense Acquisition University, and Defense Systems Management College,* Defense Systems Management College Press, Fort Belvoir, Va., May 1999.
3. *NRO Acquisition Management Directive 7* (NROD 82-2, OPR (P&A), National Reconnaissance Office, Aug. 6, 1997. Available on the web at http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.html
4. Loveland Link, Jo Lee, Rick Barbour, Al Krum, and August C. Neitzel, *Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office,* CMU/SEI-99-T R-009, ESC-TR-99-009, SEI Technical Report, December 1999.
5. Schein, Edgar H., *Organizational Culture and Leadership,* Jossey-Bass Business and Management Series, San Francisco, 1997.
6. Neitzel, August C., Jr., *Managing Risk Management,* CROSSTALK: July 1999.
7. *IMINT Malcolm Baldridge National Quality Award Assessment Consolidation Report,* National Reconnaissance Office, May 1996.

About the Authors

August Neitzel is Director, EIS Ground Group, responsible for system delivery. During the period of risk management rollout and installation, he was division chief of IMINT's command and control acquisition effort. In this capacity, he led the pilot program for the initial IMINT risk management initiative. In addition, he served as the contracting officer's technical representative for the command and control acquisition contract. Neitzel joined the CIA in 1975. In 1982, he began working for the NRO. His career there has spanned the SIGINT program and virtually all aspects of the IMINT program. Neitzel earned a master's degree in electrical engineering from Drexel University after completing a tour of duty with the Air Force. He is a member of Eta Kappa Nu and the Institute of Electrical and Electronic Engineers. He is certified as a Level III COTR, and received the CIA Intelligence Commendation Medal.

NRO
4101 Pleasant Valley Road
Chantilly, Va. 20151
Voice: 703-808-2038

Jo Lee Loveland Link is a visiting scientist at SEI, with more than 20 years of providing guidance for strategic direction of government, military, and private sector organizations. For the past six years, she has worked with technical programs to establish strategy and infrastructure for process improvement and risk management initiatives. With Richard Barbour, she provided risk management rollout and installation services across this IMINT organization. She has participated on Capability and Maturity Model®-based assessment teams and teaches several SEI workshops, including Managing Technological Change, Consulting Skills, and customer-tailored Risk Management. A certified Senior Organization Development and Change Specialist with post-graduate work in applied behavior science, Loveland Link has a bachelor's degree in organization behavior/adult education, and is author of more than 30 publications on strategic planning, management, and corporate culture.

Software Engineering Institute
4301 Wilson Blvd., Suite 910
Arlington, Va. 22203
Voice: 703-709-9217 or 703-908-8232
Fax: 703-904-8330
E-mail: jll@sei.cmu.edu

Richard E. Barbour is a senior member of the technical staff at CISE. For the past year, he has provided software capability evaluations (SCEs) to international software companies. In 1998-99, Barbour was instrumental in SCE assessments for the NRO future imagery architecture program. Prior to joining CISE, he was in the SEI software engineering process management program as the acquisition improvement project leader, serving as lead for the SEI-NRO risk management initiative. He had been in the SEI Process Program, developing and implementing Capability Maturity Model®-based appraisals for internal process improvement and software capability evaluations. He also spent a year with the SEI Transition Partner, Integrated System Diagnostics Inc., developing the SCE v. 3.0 method. Barbour has more than 24 years of experience in managing and acquiring software systems, and is a retired Navy Commander from the antisubmarine warfare, patrol squadrons (P-3) community. His last assignment was as deputy program manager for the Next Generation Computer Resources program with the Space and Naval Warfare Systems Command. He also was deputy program manager for the Software Technology for Adaptable, Reliable Systems program. He received a bachelor's degree in business management from the University of South Carolina, and a master's degree in computer systems management from the Naval Post-Graduate School.

CISE
4516 Henry Street, Suite 205
Pittsburgh, Pa. 15213
Voice: 412/268-4312
Fax: 412-268-6369
E-mail: reb@cise.cmu.edu

Al Krum is Director, Systems Engineering Sector, IMINT, NRO. At the time of the Risk Management Rollout and Installation, he was Program Director, Enhanced Imagery System (EIS), IMINT.

Risk Management Web Sites

www.eas.asu.edu/~riskmgmt This is Arizona State University's (ASU's) software risk management home page. Links include an introduction to software risk management, risk identification questionnaire, and a risk management expert system.

www.infc.ulst.ac.uk/informatics/ise/se/re/serum.html Software Engineering Risk: Understanding & Management (SERUM) site.

www.ida.liu.se/labs/aslab/people/joaka/risk_bib.html Software risk management bibliography with a compilation of software risk management articles by Barry Boehm, R.N. Charette, R. Fairle, et. al.

www.esi.es/Information/Collections/SoftRisk/tools.html Software Risk Management: Tools, including links to risk track, NASA Software Risk Management Database, Software Acquisition Capability Maturity Model®, v. 1.01, and Risk Management Tutorial.

www.spmn.com Software Technology Conference '99 presentations, May 3-6, allows users to download .ppt files on *16 Practices for Improving Software Project Success* by Jane Lochner, and *Software Process Improvement at PMW-163* by Frank Doherty. Also includes Software Program Managers Network quick links.

www.sei.cmu.edu/legacy/risk/kit/metrics.html This focuses on conveying software development risk status without sending upper management into a panic.

www.rollanet.org/~asemmsd/em-handbook/Abstracts/rsk_tool004.html Abstracts on risk management

www.sea.net.au/project_management/risk_management International links on:

- Software risk evaluation service and risk management overview from the Software Engineering Institute.
- ASU's software risk management home page.
- Cost of Risk Analysis System by International Security Technology Inc.
- Mesa/Vista Risk Manager, a collaborative web environment that provides the foundation to support a structured risk management process.
- Department of Defense Data Analysis Center for Software site with case studies, resources, training, discussion groups, software tools, and FAQs.