Managing Risk Management

August C. Neitzel Jr.
National Reconnaissance Office

This article will address the development of a pilot risk management effort within the National Reconnaissance Office's Imagery Intelligence Systems Acquisition and Operations Directorate (IMINT). The topics to be covered will be the background and rationale for the instantiation of a risk management program and the working relationship with the Software Engineering Institute in tailoring its processes that led to the development of an automated Risk Management Tool. The methodologies and processes in place, as well as lessons learned and future follow-on efforts also will be addressed.

Background

The National Reconnaissance Office (NRO) underwent a consolidation and collocation of its resources to northern Virginia from late 1993 through early 1994. This brought together, for the first time on a large-scale, members of the NRO uniformed services and the Central Intelligence Agency.

In March and April 1996, the director of the NRO commissioned a Baldridge study to assess the quality of life and the processes in place in the NRO. The study addressed a broad spectrum of topics. The results indicated issues existed in the acquisition and planning processes, communications, and personnel. These issues were, to a large extent, due to cultural differences of the newly combined military and civilian organizations.

While other elements of the NRO addressed the wider NRO Baldridge issues of communication and personnel, the NRO's IMINT focused on its internal acquisition and planning processes. To facilitate this focus, IMINT requested that the Software Engineering Institute (SEI) from Carnegie Mellon University, a federally funded research and development center (FFRDC), conduct its Software Acquisition-Capability Maturity Model^{SM} (SA-CMM) [1] survey of IMINT. IMINT's goal was to achieve an overall improvement in its acquisition processes.

Starting in August 1996 the SEI conducted the IMINT SA-CMM. The SA-CMM survey allowed the SEI to interview a broad cross-section of IMINT's government and contractor (i.e. development, FFRDC, Contractor Advisory and Assistance Services, and System Engineering Technical Assistance) personnel. The results of the survey and the Baldridge study were fairly consistent in the area of process improvement.

Although the SEI SA-CMM survey identified many strong acquisition process areas (e.g. rigorous configuration management, development standards, and acquisition methodology) it found weaknesses in the uniform application of the established processes to the acquisition of NRO's systems. Risk management was a notably weak area. In this case the government program office had no documented processes to follow. This was in stark contrast to IMINT's contractor community, which in general had very proactive and rigorous risk management programs in place.

The briefing to IMINT management by the SEI SA-CMM team concluded that IMINT should embark on an acquisition improvement program, with an emphasis on establishing a Team Risk Management (TRM) program. More specifically, the SA-CMM team recommended forming a pilot TRM program. IMINT management adopted the recommendation.

IMINT management's rationales for needing a strong risk management discipline are the same as those shared by most of their Department of Defense (DoD) and industrial mission partners. As systems become more complex and interactive, it is essential to identify and understand the interrelationship of the risks within and across programs. The programs must appreciate how a risk in one element may cause a risk in another element. Risks that are not proactively managed eventually begin to manage you. Early risk assessment and mitigation can and will minimize downstream surprises and problems. Shrinking budgets and tighter schedules virtually eliminate any margins that could be retained to offset problems that might occur late in a program.

Following the SEI SA-CMM recommendation, IMINT management selected its command and control development (CCD) effort, for which the author is the program manager, as the vehicle for the pilot TRM program. This selection was made in part because the CCD effort is the most software-intensive acquisition program within IMINT and the NRO, and in part because there was some degree of belief that the SA-CMM process was primarily applicable to software development efforts. The CCD acquisition consists of several million lines of code (new, modified, and reuse) and utilizes C++ object-oriented design (OOD). It is commercial-off-the-shelf products (COTS) intensive and is a large distributed client/server architecture of several hundred servers and workstations. It has multiple deliveries spanning more than three years and over geographically dispersed facilities. In addition to the software sizing aspects of the CCD effort, there was some degree of the “let Mikey try it” syndrome in IMINT's decision. The author being viewed as the resident skeptic, IMINT management seemed to think that if CCD bought into the TRM process, others would readily follow. On this ceremonious note the pilot program was off and running.

Software Acquisition-Capability Maturity Model (SA-CMM) is a service mark of Carnegie Mellon University.

The Pilot Team Risk Management Program

The first step was to reconvene a SEI/contractor/government team and establish a plan of attack. CCD elected to initially limit the scope of the pilot program to a subset of their overall acquisition activities. The CCD acquisition effort had several incremental deliveries in its plan. One of the later deliveries was selected as the basis for the pilot effort. This later delivery involved one of our subcontractors who was chosen to be the primary participant in the study, with our prime contractor providing a supporting role. The driving rationales for this were multifaceted. The main one was to minimize any potential disruption to more time-critical activities. Another was to select an activity early enough in its acquisition process that it might better accommodate any potential change. A third was to select an activity where the cultural differences were the most noticeable.

CCD initiated its SEI-led Software Risk Evaluations (SRE) in January 1997. The CCD contractor was chosen to begin the process and conducted its own, separate Risk Identification and Analysis (RI&A) and Mitigation Strategy Planning (MSP) phases in two five-day periods concluding in March 1997. The CCD government team immediately followed with its own SRE RI&A and MSP phases in April and May 1997. The contractor and government SREs were done separately to ensure confidentially and to build a baseline of risks to be selected by both organizations for joint mitigation in a TRM environment.

The CCD program office's RI&A portion of the SRE involved four independent teams. Members of CCD technical staff (i.e. area managers) made up team one, CCD management made up team two, members of CCD's Aerospace FFRDC cadre made up team three, and members of CCD's operational customers and systems integration contractor made up team four.

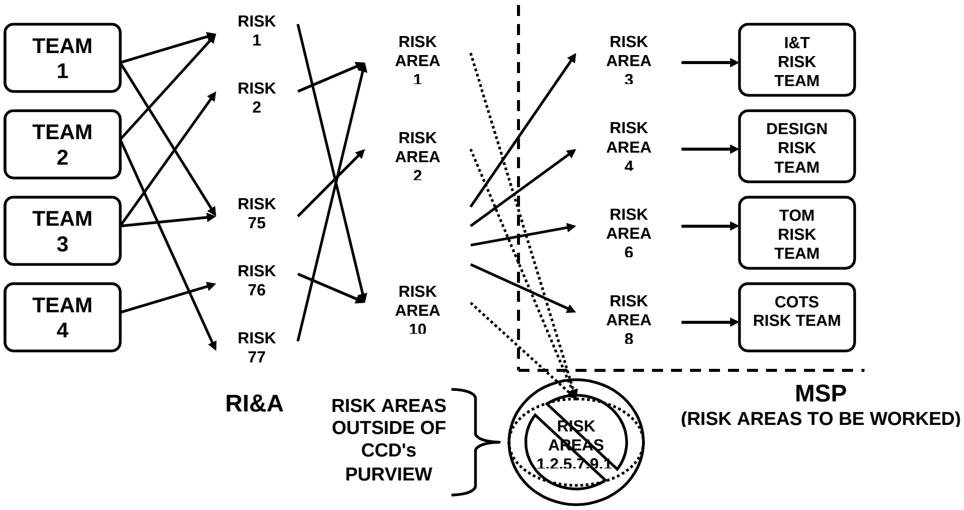
Each of the four RI&A teams utilized the SEI SRE taxonomy questionnaire. The four teams generated 77 risk statements. In some instances a risk statement was unique to a team. In other cases, multiple teams generated the same risk statement. SEI compiled and tabulated the 77 statements and assigned them into 10 risk areas or affinity groups. The 10 areas and the number of risk statements generated within each were:

Risk Area 1 — Requirements (11)
Risk Area 2 — Staffing (7)
Risk Area 3 — Integration and Test (I&T) (7)
Risk Area 4 — Design (8)
Risk Area 5 — Schedule (3)
Risk Area 6 — Transition to Operations and Maintenance (TOM) (7)
Risk Area 7 — Program Office Management (16)
Risk Area 8 — Commercial-off-the-Shelf products (7)
Risk Area 9 — Prime/Subcontractor Relationships (4)
Risk Area 10 — Contract Management (7)

The joint TRM process commenced in June 1997 with a government/contractor/SEI MSP session. The joint team chose to pursue Risk Areas 3, 4, 6, and 8 for mitigation. A risk team was assigned each of the selected risk areas for further characterization and mitigation strategy development. It was thought that these four areas would provide more than enough risks to attempt to mitigate in a pilot program. In addition, it was thought that the other risk areas (1, 2, 5, 7, 9, and 10) fell outside the purview of the CCD team and the probability of successfully mitigating any of the associated risks was low and of minimal payback. For instance, in the area of requirements, most of the requirements' instability risks were driven by external elements to either CCD or IMINT. The likelihood that the CCD team could unilaterally control the flow of changes was improbable. Interestingly though, these areas subsequently were assigned and worked at a higher management level when the CCD risk management process was adopted at the IMINT program development level. Figure 1 provides a representation of the RI&A and MSP process CCD followed.

The area of risk training was a key aspect in the development of the CCD pilot TRM program. The CCD team took advantage of the SEI risk training that stepped us through the SRE RI&A and MSP, Continuous Risk Management (CRM), and TRM concepts. However, we elected to skip the risk clinic training SEI offered. We thought (incorrectly) that the details taught in the clinic were unnecessary and we already knew what we needed to know to succeed. As we progressed through the various risk management stages and attempted to develop our pilot plan, we soon came to the conclusion that the risk clinic was a valuable tool we should not have been so cavalier in discarding. The team found it was having difficulty with not only the risk management lexicon but also in developing a firm understanding of what differentiated a risk from an issue/problem. With our belated participation in the risk clinic, we discovered that the team members inherently understood the steps each was tak-

Figure 1. Software risk evaluation process.



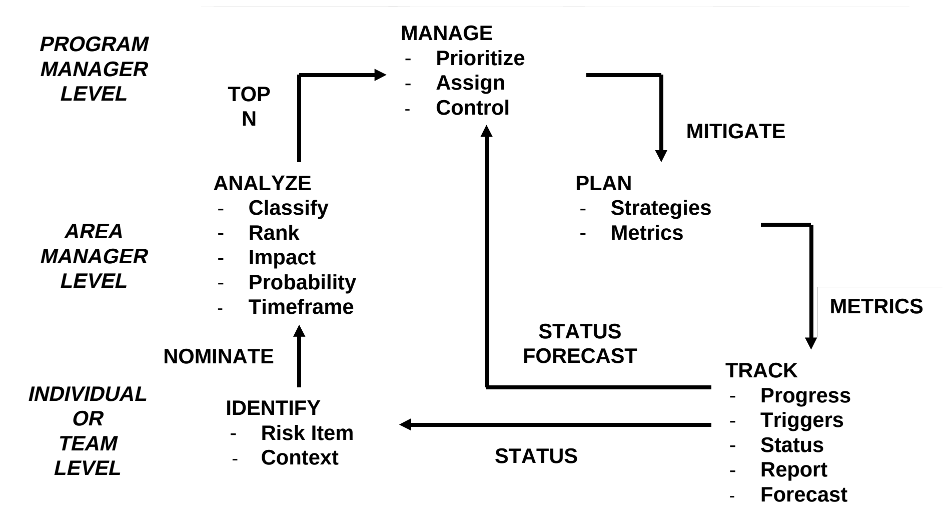


Figure 2. Continuous risk management flow.

ing to identify, quantify, and mitigate risks. The problem was in establishing a documented and uniform process that the entire team could follow. We utilized the CRM flow concept that is documented in SEI CRM handbook [2] and tailored it to fit our process flow.

In the CRM process we developed for our pilot program, we allocated responsibility for the initial identification of a risk to the teams and individuals most readily familiar with the program element. It is the function of these individuals/teams to define the risk item and put it in a context that clearly categorizes it.

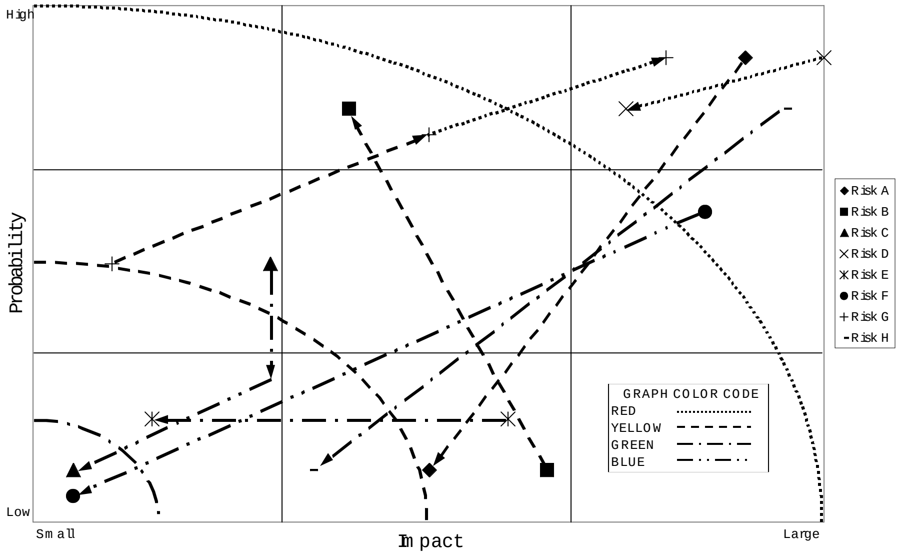
These risks are passed on to the CCD area managers, who analyze them to determine the potential impact, probability, and timeframe of occurrence. The area managers then proceed to classify the risks according to impacted area, closure criteria, decision timeframe, and response. In our adaptation of the CRM flow, we added "support" to the existing responses of watch, accept, and mitigate. There are numerous instances where an IMINT risk is present for which CCD would have no mitigation responsibility, but where CCD support would be needed for formulating an adequate mitigation plan. If the area managers chose to accept the nominated risk, they rank its significance relative to all the risks under their purview and pass the top N to CCD management for ultimate prioritization, assignment, and control (i.e. disposition).

CCD management then has the option of modifying any of the risk parameters (e.g. probability, decision timeframe, and impact) and placing the risk in the CRM plan. Once in the CRM plan, the appropriate mitigation strategies are developed along with the metrics needed to assess progress against the plan. The tracking system allows for routine progress and status reports to be generated, as well as producing briefing material to identify current status and forecast future movement. Trigger points are established to alert management and the risk manager of key decision dates or activities for the risk in question. Figure 2 shows a top-level representation of the CCD risk management flow.

The team developed two significant risk-reporting presentations used in briefing senior IMINT management. The first report is a barometric-like representation that tracks our risks throughout the impact — probability continuum. This gives senior management a snapshot of where risks have been and where they are going at a top level. Figure 3 provides an example of our barometric chart. The curved lines that connect the impact and probability axes provide a quick visual assessment of the risk groupings.

The second report, which is still a work in progress, assesses the exposure the program faces on any given risk. This report melds the risks' impact and probability values along with the decision timeframe, budgetary, and Technical Performance Measurands (TPM) factors for a visualization of the risk population's relative exposure. TPMs are a measurement of those items that the NRO has committed to provide its customers. For example, given two risks with equal impact, probability, and decision timeframe, the one that is unbudgeted and adversely affects a TPM probably deserves more management attention than one that is budgeted and has no impact on a TPM. Figure 4 shows an example of the prototype exposure report. In this example, Risk F is ready to be closed, and CCD's second highest priority risk, Risk A, has lower exposure than the next highest exposure risk, Risk G. The implication is that the next level of management probably needs to apply more attention to Risk G than Risk A. In practice, Risk G might fall into a "watch" or "support" category for CCD but into the "mitigate"

Figure 3. Risk barometric chart.



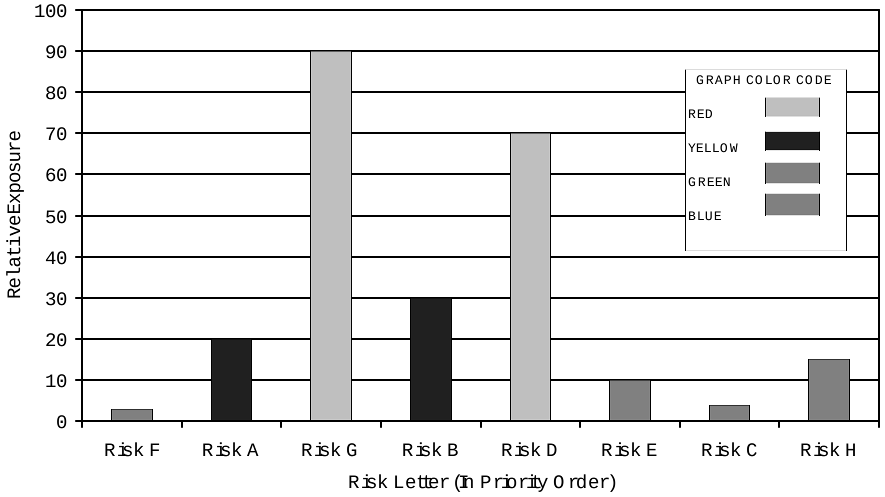


Figure 4. Risk exposure.

category for IMINT at large.

(Note: Figures 3 and 4 are typically represented in a four-color format with red representing items with the greatest risk and exposure through blue for those that are of the least risk and exposure and ready for closure. The figures include a Graph Color Code key for identifying the color scheme in the black and white figures.)

In conjunction with formalizing and documenting the risk process flow, we also established dedicated meetings with formal agendas to nominate and disposition risks within CCD. Each Monday the area managers review and status the risks they are managing. Monthly, at our joint Team Risk Reviews (TRRs) with our contractors, and facilitated by SEI, new risks are nominated, mitigation plans are developed, and old risks dispositioned. We have found it extremely beneficial to have a broad government/contractor/SEI experience base at these TRRs, as it produces a superior mitigation plan.

The Risk Management Tool

We continued to refine and enhance our processes as the CCD pilot risk team progressed through the various phases of the SEI process. One of the more significant products was the development of our Risk Management Tool (RMT).

The RMT is the result of a collaborative team effort between the CCD, government, Lockheed Martin Corp., and ORACLE.

The team's objective was to model the SEI/CCD CRM process established during CCD's risk clinic and to develop an automated interactive Web-based tool — the RMT.

The RMT facilitates a hierarchical approach to propagate risks through the system by enforcing workflow via defined roles and responsibilities for all users. The RMT's assignment feature provides users with the capability to communicate with other users in the system and to move risks through the approval processes. Personnel is notified of risk assignments via automatically generated e-mail. Personnel associated with a risk also is notified via system-generated e-mail when key data items are added or updated.

The RMT's built-in security features provide data protection and partitioning that prevents unauthorized access and enforces the defined hierarchical workflow.

The tool engages the end user with its intuitive graphical user interface (GUI). GUI features include JavaScript-assisted pop-up lists, pull-down menus, and free-form data entry fields. JavaScript also is employed to perform client-side validation of user entries. The user-friendly RMT includes detailed online help and real-time validation checking. Numerous custom query screens and reports provide valuable information on risk status and progress measurement to support decision making. Reports are provided in either textual or graphical format, including the barometric and exposure reports discussed earlier.

The tool is designed for use with a risk-management methodology modeled after the SEI process. When used in conjunction with other established program management processes such as earned value management and critical path methodology, it greatly enhances insight into the acquisition process for program management.

Success Stories

The pilot TRM program developed by IMINT CCD has been successful and forms the basis for the larger TRM program that spans all the acquisition activities within IMINT. The CCD processes provided the foundation for the acquisition activities' Executive System Risk Team (ESRT), which convenes monthly and is chaired by the program director. This forum assesses the most significant risks facing the program and concentrates on the interdependent risks. Many of the risks that CCD identified in the RI&A phase of its pilot program, which were out ofits mitigation purview, now are managed within the ESRT.

In developing the TRM process and propagating its use across the various development disciplines, we refuted the concept that the SA-CMM methodology is limited to software acquisition programs. The "S" in SA-CMM might more accurately stand for "systems" as opposed to "software".

Work is under way to expand the risk program into IMINT's operational elements, although operational personnel do support the ESRT.

CCD has been asked to share its TRM experiences and lessons learned with the NRO's Acquisition Steering Group and Signals Intelligence Acquisition and Operations Directorate (SIGINT) to aid them in the development of their own TRM efforts. Additionally, SEI and CCD have worked with the NRO's Acquisition Center of Excellence to promulgate a TRM concept across the larger NRO community.

A contractor for one of the NRO's biggest customers, The National Imagery and Mapping Agency (NIMA), has asked to utilize the processes that CCD developed in formulating its TRM program. On a more basic level, the TRM program is proving to be of greater and greater utility as IMINT's programs progress through the acquisition phases and near its operational readiness milestones. The formalization of the risk process has helped to develop a higher confidence level for senior management. They now have better access to and greater insight into the interrelationships of the key development activities. As each of the interlocking development programs have embraced a TRM process, a clearer picture has materialized that shows how tightly coupled these activities are. Not only has senior management's visibility into previously obscure details improved, but other contracting officer's technical representatives within the program have a better appreciation of how risks within its sphere of influence might impact others in very subtle ways.

The development of the TRM program has provided a mechanism for early risk identification and mitigation. This proactive approach allows IMINT to place its risks in better perspective and to focus on those with the highest potential (i.e. greatest exposure) to negatively impact the programs' process. By thoroughly defining and quantifying a risk's potential impact, it has been possible to establish budgetary liens that have withstood detailed scrutiny.

A side benefit is that the government/contractor team has forged a much closer and candid working relationship. The ability to bring together key talents and a broad experience base from the combined government and industry sides of the acquisition process has enhanced both participants.

Lessons Learned

The first lesson that all the participants quickly became aware of was that we should not have bypassed the SEI risk clinic. Although the team inherently understood the basic risk identification thought processes, it was essential that we develop a common lexicon and work through the risk identification formality. The TRM plan and risk process flow that resulted from our participation in the clinic allowed us to further enhance our processes as management requirements have changed.

Some in the organization still treat a risk as a four-letter word. The key is that risks are a natural byproduct of any activity. The more complex and challenging the effort, the greater the inherent risks. Managers need to recognize this and not hesitate in bringing risks forward to senior management. Likewise, senior management should not "shoot the messenger," nor should senior management be over-eager to help. Intervention is likely to restrict the open flow of information.

Differentiating a risk from a problem is still difficult for many. It is essential in the TRM process to identify potential problems and bring them to light as soon as practical. To do otherwise is unproductive. The exchange of information is severely restricted and the ability to develop comprehensive mitigation plans is inhibited.

For the TRM process to work, senior management must buy into the process. It is essential that the management team devotes the necessary time and energy to the process and continually reinforces the required discipline.

The establishment and execution of a CRM process requires a reasonable expenditure of resources. The CCD team spent many hours establishing its process and developing its risk database. The effort needed to maintain the momentum is considerably less, but by no means zero. Our weekly area manager meetings and monthly TRR and ESRT meetings continue to require support to be viable.

Lastly, as the team progressed through the process, we realized that risk management does not stop when an element is transitioned to operations. It is important that operational risks also are managed. In keeping with this recognition, our Integrated Development and Maintenance Organization (IDMO) instituted a risk management process that helps to better focus and prioritize available resources. Our IDMO is actively represented on our TRRs and ESRTs.

The Future

The challenge from NRO management to the team is to quantify the successes that a proactive TRM program can bring to an organization. Although both the CCD team and now the IMINT programs team can point to clear examples of where the risk program has helped identify and mitigate risks, we have not yet established a set of metrics that allows us to quantitatively represent the successes.

The risk barometric graphic (Figure 3) has been very useful in quantifying the progress on any individual risk from inception through retirement, but in itself is not adequate.

The CCD team is investigating the utility of tracking a risk's exposure as a function of time to see if this, coupled with the barometric representation, provides any additional insight. As we continue to enhance our data collection and reporting in this arena we hope that it will address the challenge we have been given. ◆

References

1. Software Acquisition-Capability Maturity Model (SA-CMM) V1.01 (CMU/SEI-96-TR020)
2. *Continuous Risk Management Guidebook*, CMU/SEI, October 1996.

About the Author

August Neitzel earned a master of science 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 joined the Central Intelligence Agency (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. He is chief of IMINT's command and control acquisition effort and the contracting officer's technical representative for the command and control acquisition contract. He is certified as a Level III COTR by the CIA. Neitzel received the Intelligence Commendation Medal for his work with the CIA.

Voice: 703-435-7217
Fax: 703-808-2038
E-mail: neitzela@nro.mil