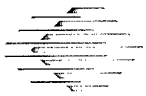


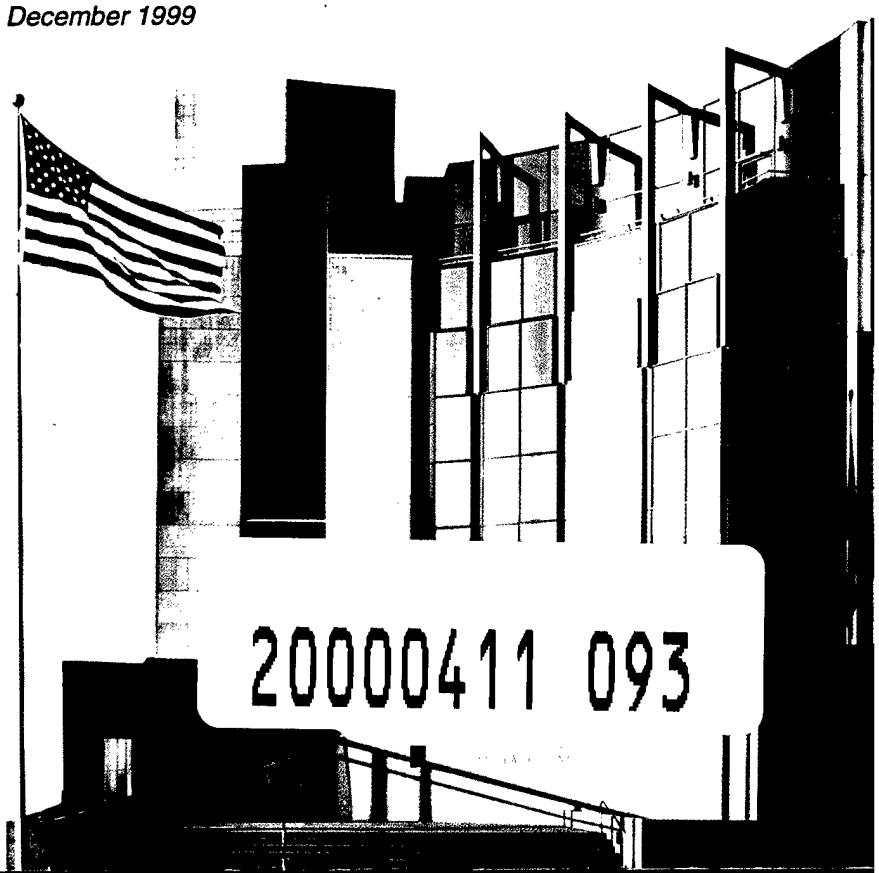
Carnegie Mellon
Software Engineering Institute

Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office

Jo Lee Loveland Link, NRO Technical Team
Rick Barbour, NRO Technical Team
Al Krum, Director of the EIS Program
August C. Neitzel, Command and Control Division Director

December 1999

TECHNICAL REPORT
CMU/SEI-99-TR-009
ESC-TR-99-009



Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of "Don't ask, don't tell, don't pursue" excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office

CMU/SEI-99-TR-009
ESC-TR-99-009

Jo Lee Loveland Link, NRO Technical Team
Rick Barbour, NRO Technical Team
Al Krum, Director of the EIS Program
August C. Neitzel, Command and Control Division Director

Principal Contributors:
National Reconnaissance Office: Lt. Col. Mike Rhodes, Paul Albright, Tanya Wilkerson
Tommy Meeker
Software Engineering Institute: Audrey Dorofee

December 1999

Software Engineering Process Management Program

This work is sponsored by the National Reconnaissance Office.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Acknowledgments

The *Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office,* which has been produced as a technical report by the Software Engineering Institute (SEI) has been developed as a result of collaborative efforts between IMINT and the SEI. This collaboration has been guided by the strategic partnership between the NRO and the SEI, as described in the preface to this report.

In keeping with the collaborative intent of the NRO/SEI partnership, the *Rollout and Installation* report is co-authored by a team of four: two NRO leaders who were pivotal in the Risk Management initiative, and two key members of the SEI technical team. All four authors worked together on the IMINT Risk Management initiative. The author team includes NRO leaders Al Krum, who was EIS Program director during most of the rollout and installation initiative, and Gus Neitzel, who was division chief of the Command and Control Division, the initial pilot site for the Risk Management. SEI co-authors include Rick Barbour, who was project lead for the Risk Management rollout and installation at IMINT, and Jo Lee Loveland Link, who served as the SEI Risk Management coordinator for IMINT. The co-authors worked in close partnership during the rollout and installation to support successful results.

The IMINT Risk Management rollout and installation initiative clearly reveals that the dedication of many contributes to the success of many others. The author team acknowledges a debt of gratitude to many devoted individuals from both IMINT and the SEI, who have contributed generously in rich and diverse ways to both the IMINT Risk Management initiative, as well as to this report. This point is important, because any effective Risk Management effort inherently includes and welcomes multiple perspectives.

To represent the IMINT Risk Management initiative as fully and fairly as possible, the authors purposely involved many voices and many views in the development of this document. The purpose of this approach was to assure that the report process applied one of the core principles of Risk Management: involvement of multiple perspectives. Therefore, the report relied heavily on interviews with IMINT practitioners across the organization, including IMINT contractors.

Interviews were graciously provided by IMINT contributors Lt. Col. Mike Rhodes, Paul Albright, Tanya Wilkerson, Tommy Meeker, Kevin Wardlow, Frank Warakowski, and Jon Katz. Their insights, candor, and willingness to share both successes and challenges were invaluable to the production of this report.

These IMINT contributors also provided in-depth document review. In addition, SEI reviewers gave generously of their time and made suggestions for improvement of the report, including Bill Peterson, Jon Gross, Brian Gallagher, Julia Allen, Linda Levine, Lisa Brownsword, and Frank Cisti.

The Risk Management initiative was successfully launched because of strong sponsorship by IMINT leadership, and diligence by IMINT and SEI project team members. Fred Dubay and then-EIS Director Fred Doyle, with guidance from Brig. Gen. Robert E. Larned, launched the NRO SA-CMM assessment, which led to the Risk Management initiative. Loren Brandman, as the original IMINT coordinator for these efforts, devoted hours of conscientious attention to the launch.

Foremost among initial SEI contributors were Gene Bounds, the original program director; Bob Holibaugh, project lead; Larry Jones; and others. Julia Allen, SEI program development lead, provided guidance to the overall initiative and supported NRO Deputy Director Dave Kier in crafting the NRO/SEI strategic partnership. Currently led by NRO Project Director Brian Gallagher, ongoing SEI efforts receive contributions by SEI Process Improvement Team members John Waclo and Ray Williams, with ongoing support by current SEI Program Development Lead Scott Reed, and Program Coordinator Jan Morgan.

Special acknowledgment is due the IMINT Command and Control Division (CCD), led by Gus Neitzel. CCD served as the pilot Risk Management program for IMINT. Appreciation is especially due to the members of the CCD Team Risk Review, who actively contributed to and sustained the success of Risk Management in this division and across the entire IDP organization. These pioneers include Charley Meadows, Melanie Camp, Roseanna Gilbert, Creed Morgan, Tracy Duggan, Kevin Wardlow, Milton Harrison, Richard Meier, and earlier, John Schiphorst, Ron Moeller, and Ron Hooper.

Additional significant contributions from within IMINT to the Risk Management initiative were provided by the Development Systems Division, including Rob Moore, then-director of the division, as well as Dan Wright and Patti Reynolds.

Appreciation is also extended to the SEI Risk Management Program members who contributed years of dedication, hard work, and resourceful solutions to the training, publications, guidance, methodologies, tools, and templates that were available as assets for the IMINT Risk Management rollout and installation. This report draws significantly on their collective thinking and high-quality materials. Members of the Risk Program were responsible for developing the *Continuous Risk Management Guidebook*, the Risk Management training, the Risk Clinic methodology, the Software Risk Evaluation methodology, and other supporting methodologies and materials. The central Risk Management team included Audrey Dorofee, Julie Walker, Jodi Horgan, Ray Williams, George Pandelios, Dick Murphy, Rick Barbour, Chris Alberts, Sandy Behrens, and Pam Williams. Rick Barbour provided leadership to special initiatives and ultimately accepted leadership of SEI Risk Management efforts.

A most special debt of gratitude is extended to Ron Higuera, who was program director for the Risk Management Program for three years, and who provided generous, visionary, and dedicated leadership and mentoring to us all. Without his contributions, none of these efforts would have been possible.

Finally, the coauthors would like to express our heartfelt appreciation and debt of gratitude to the SEI Technical Communication team, led by Bill Thomas, senior writer/editor for this technical report, together with senior writer/editor Claire Dixon and graphic designers Mark Paat and Bob Fantazier. The coauthors were provided with excellent editorial and design guidance, important improvements, and writing for certain passages.

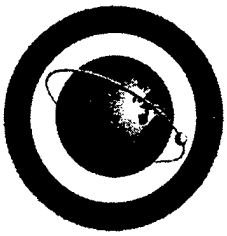
The "dedication of many" has been joined by the active Risk Management practitioners at IMINT, who have become part of an evolving learning community. The advancement of Risk Management translates to advancement of the quality, resilience, rigor, and success of critical mission systems. Risk Management undergirds and sustains the ability of these important systems to continue providing essential security for the United States and the world.

Therefore, these acknowledgments include appreciation for all those new Risk Management practitioners who, in a continuous community of learning and practice, in turn become mentors and supporters of others.

Jo Lee Loveland Link
Rick Barbour
Al Krum
August C. Neitzel

Preface

A letter from David A. Kier, deputy director of the National Reconnaissance Office, follows.



NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

Office of the Deputy Director

The National Reconnaissance Office (NRO) has a long history of excellence in production of advanced technology systems to provide the highest levels of information for the nation's security, to support our military in achieving mission success, and to help assure the security of the American people. The NRO vision, "Freedom's Sentinel in Space: Revolutionizing Global Reconnaissance," is a living pledge: the NRO is committed to remaining a leader in finding solutions to the ever-increasing demands of technological superiority in the new century. Joint Vision 2010 forged by the Joint Chiefs of Staff is predicated on information superiority.

To achieve our compelling aim, the NRO must produce the best programs, while addressing the growing challenges of developing and launching complex systems in an era of rapid technological change and a more multifaceted, complex global environment. The demands for high levels of information quality and security have never been greater. Technological advances demand agile and flexible management techniques in order to continue to provide timely, high-quality intelligence. At the same time, the NRO is committed to optimum use of our resources. We are consolidating programs, while seeking greater cost efficiencies with no loss of effectiveness in critical capabilities.

In support of these goals, in May 1998 the NRO entered into a strategic partnership with the Software Engineering Institute. The intent of this partnership is to collaborate in defining strategic areas of focus that will support improvements in acquisition, risk, and program management for the NRO, and to leverage joint initiatives to support these strategic areas.

The first of these initiatives was the rollout and installation of Risk Management for the Imagery Development Program at the Imagery Intelligence (IMINT) Directorate of the NRO. IMINT's acquisition strategy is based on becoming more efficient in acquiring and managing complex systems, with Risk Management as the key to continued improvement. Risk Management has successfully provided IMINT with opportunities to gain and exploit greater insight into choices and tradeoffs that must be made in acquiring, building, and operating systems. Partnerships between government and contractors have resulted in the proactive and robust management of risk. Information about technology and schedule risks and problems has been communicated to management better than ever before, allowing for more rapid strategic response and replanning when necessary.

These achievements are real and vital. The promise of risk management can be realized—and improved—for the future development of our systems. NRO leadership encourages Risk Management throughout all of our programs, to ensure the increasing level of excellence that is our pledge.

David A Kier
Deputy Director
National Reconnaissance Office
December 1999

Executive Summary

This report on the *Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office,* has been produced as a technical report by the Software Engineering Institute (SEI) as a result of a collaborative effort between the Imagery Intelligence (IMINT) Directorate of the NRO and the SEI. Beginning in 1997, the NRO's leadership agreed to enter into a strategic alliance with the SEI. This alliance began a partnership between the two organizations to work together as the NRO faced the 21st century's technological and mission challenges. The Risk Management pilot project, and subsequent rollout and installation, were launched in the Imagery Development Program (IDP) at IMINT.

Report Timeframe and Purpose

The timeframe of the report begins with the Software Acquisition Capability Maturity Model® (SA-CMM®) assessment conducted during the winter of 1996–97 and the initial Software Risk Evaluation (SRE) conducted during the spring of 1997, up to the merger in May 1999 of IDP with the Future Imagery Architecture Program, resulting in the current IMINT Development Program (IDP).

The central purpose of the report is to provide a knowledge asset repository for the National Reconnaissance Office that can be leveraged in support of further Risk Management efforts.

Background of the Risk Management Initiative at IMINT

Coupled with the Jeremiah findings from an earlier blue ribbon panel report commissioned by NRO Director Keith Hall (the "Jeremiah" findings), there was a growing conviction by IMINT leadership that previous methods of management and operations would not suffice to assure IMINT strong entry into the 21st century. Programs were forging multiple mission partners and customers into cohesive program delivery systems that could promise and assure successful results, while at the same time requiring deft integration of multiple perspectives and requirements.

Accordingly, IMINT leaders explored best practices and options to enhance program effectiveness for the organization. Seeking to leverage the established track record of the SEI in improving defense and civil federal organizations, initial contact was made by the NRO with the SEI at the SEI Information Day in 1995.

® Capability Maturity Model and CMM are registered in the U.S. Patent and Trademark Office

The IMINT SA-CMM Assessment and the Decision to Pursue Risk Management

Understanding that significant savings and technical reliability for mission-critical systems would be enhanced by acquisition excellence, IMINT leaders actively pursued best approaches to modernize and improve operational capability. They decided to conduct the SEI SA-CMM assessment to determine strengths and gaps in their capability as an acquisition organization. The SA-CMM assessment findings identified a number of areas for improvement opportunities at both Level 2 and Level 3 of the SA-CMM model.

Notably, the NRO lacked a consistent, rigorous, documented Risk Management practice. This finding was validated by NRO leaders; they observed that their insight into future risks, and the level of unexpected program difficulties, were unacceptable. In fact, several times catastrophic problems occurred without warning, and resources had to be diverted to correct problems that could have been avoided or reduced in severity if the risk had been known in advance. In addition, NRO leaders were aware of growing support and urgency for Risk Management from the Department of Defense, the General Accounting Office, civil agencies, and industry.

Accordingly, from among the potential SA-CMM improvement areas, IMINT leaders determined that the optimum first initiative would be Acquisition Risk Management (a Level 3 key process area), which could provide immediate strategic and tactical support for IMINT programs. Risk Management promised the opportunity for IMINT to develop an intrinsic capability to surface, address, and mitigate preventable problems throughout program life cycles.

Launching Risk Management at IMINT

To launch the Risk Management initiative, IMINT leaders identified the Command and Control Division (CCD) in IDP for a pilot initiative. They further decided to conduct Software Risk Evaluations (SREs) with both the government organization and the principal contractor for CCD. The first of these two SREs was performed in January 1997 with the contractor and the second in April 1997 with the government CCD division.

In April 1997, the CCD proceeded to install a dynamic, interactive Risk Management process throughout its program, and gave that process focus and leverage through monthly CCD Team Risk Reviews (TRRs). The TRRs served as regular forums for government and contractors to identify and mitigate joint risks. The TRRs were amplified by the separate government and contractor Risk Management processes to assure capture and mitigation of risks at every appropriate level.

Expanding from Pilot Project to System Risk Management across IDP

IDP Director Al Krum observed the effective process installed in CCD as a result of the pilot Risk Management project, and directed that similar Risk Management processes would be installed throughout IDP. To implement his decision, Risk Management training sessions were delivered to each division, and the majority of divisions also held Risk Clinics to define their Risk Management process. The consistent training across divisions assured that they developed a common language and set of tools to use internally and across the system.

Concurrently, the IDP director also launched the EIS System Risk Management Team (ESRT), with a mission to identify and address system-level risks. The ESRT membership comprised each division director, area managers, and technical specialists who could help with system Risk Management.

System Risk Management enabled members of the program, for the first time, to analyze and work together on interdependencies at the system level. Together, the divisional Risk Management processes (including contractor Risk Management) and system-level Risk Management at the ESRT were formed into a comprehensive, consistent Risk Management process that became routinely operational.

Tailoring and Standardization: Where Is the Balance?

The IDP director has said that one of his key lessons learned was that system standardization actually fosters effective Risk Management, and that if he were to "do it over," he would "establish more common methodologies earlier." The reasons for this include easing cross-system communication, accelerating joint risk mitigation planning, and assuring that key information is accurately conveyed.

At the same time, tailoring by divisions also had value. The reasons for this include aligning Risk Management with existing program management practices and methodologies, accelerating installation of Risk Management into everyday efforts, and encouraging creativity in approaches to Risk Management.

The Principles and the How-To's for Risk Management at IMINT

The report provides a fuller discussion of the core principles of Risk Management. At IDP, the system Risk Management process included all divisions and all elements of program delivery.

The core ingredients for Risk Management were broadly understood across the organization. These included

- *identifying* new risks
- *analyzing* risks
- *planning* best courses of action
- *tracking* risks
- *controlling* risks
- *communicating* throughout

The results from following this cycle, particularly the positive results of open communication, can be found in success stories throughout the *Rollout and Installation* report.

Insight into Success Factors for Risk Management at IMINT

Guidance, templates, and models for Risk Management are provided from a number of sources, ranging from the DoD to the SEI. These are sound starting points for Risk Management. In the case of IMINT, however, there is the especially valuable asset of practical, real-world experience. The resultant success factors gained through the rollout and installation of Risk Management at IDP are identified below:

1. Build Risk Management into the structure of program management and system management at the beginning. Risk Management should be integrated into overall program management. Risk Management at the division level is important but insufficient. System Risk Management that integrates all divisional efforts is essential for capturing interdependencies, interface risks, and overall priority program risks.
2. Resistance is normal and culture management for open communication is necessary; plan for both.

   Rarely is Risk Management welcomed with "open arms" in a system. Typical comments include: *"I don't have time, with all my regular project work." "Nobody wants to hear about problems that haven't happened yet." "Risk Management is too bureaucratic, complicated, and time consuming." "I don't want to look stupid, especially in front of upper management." "This is just another 'initiative du jour'—I'll wait and see if they are serious before I put any effort into it." "We already know our risks." "They* will *shoot the messenger!"* Staff are burdened already, and need to be convinced that Risk Management will help them and their program achieve success.

   A critical success factor for Risk Management is a culture of open communication and not "shooting the messenger." Or, as the IDP program director has written in the February 2000 issue of *CrossTalk: The Journal of Defense Software Engineering, "Risk management forums at both system and divisional levels are not so much places where you 'don't shoot the messenger' as where 'there is no messenger to shoot because there is not a crisis yet.'"*
3. Constancy of management support and an internal champion are musts. Leadership entails sponsorship for Risk Management—clear communication that ongoing program performance depends on proactive, future-oriented Risk Management. While Risk Management clearly leads to improved rates of program success over time, initial

investments can try the patience of staff. Strong sponsorship is needed to spur action through these tough times initially, until installation has taken hold and results become visible.

4. Contractor buy-in and collaboration enhances the adoption of Risk Management as a business process. Effective government/contractor partnership is the cornerstone of successful Risk Management in an acquisition organization. At the same time, the government retains ultimate accountability for program success. Government perspective on risks is necessarily distinct from that of contractors, and requires focused and separate attention.
5. Define all roles explicitly. Installation of Risk Management processes and practices requires development of an infrastructure, albeit a simple one. Nevertheless, clear definition of roles and expectations will go a long way toward smoothing the new initiative and assuring its success.
6. Provide a consistent set of processes and tools, and ensure their continuous use. The right balance must be struck between standardization and tailoring of Risk Management across the system, with adequate safeguards to assure consistent, streamlined, and effective risk communications and management.

In summary, we would like to quote from the SEI *Continuous Risk Management Guidebook:*

> *Risk Management is simply an area of emphasis of everyday business. It should be ongoing and comfortable. Like any good habit, it should seamlessly fit into your daily work. There is no one special set of methods, tools, or communication mechanisms that will work for every project. The key is to adhere to the principles, perform the functions, and adapt the practice to suit your needs.*

We, the co-authors, sincerely hope that this SEI technical report, *Rollout and Installation of Risk Management at IMINT, National Reconnaissance Office,* will take its place as a contribution of value in the larger body of Risk Management practice.

Abstract

The NRO Risk Management pilot project, and subsequent rollout and installation, were launched in the Imagery Development Program (IDP) at the Imagery Intelligence (IMINT) Directorate. This was preceded by a Software Acquisition Capability Maturity Model® (SA-CMM®) assessment to determine strengths and gaps in IMINT's capability as an acquisition organization. From the potential SA-CMM improvement areas, IMINT leaders determined that the optimum first initiative would be Acquisition Risk Management. To launch the Risk Management initiative, IMINT leaders identified the Command and Control Division (CCD) in IDP as the pilot initiative. They further decided to conduct Software Risk Evaluations (SREs) with both the government organization and the principal contractor for CCD. The CCD division proceeded to install a dynamic, interactive Risk Management process throughout its program, with a Team Risk Management approach. This approach was leveraged by monthly CCD Team Risk Reviews (TRRs). The TRRs served as regular forums for government and contractors to identify and mitigate joint risks.

The IDP director, observing the success of the CCD pilot, called for consistent Risk Management training across the divisions. Concurrently, the IDP director also launched the EIS System Risk Management Team (ESRT) with a mission to identify and address system-level risks. The divisional Risk Management processes (including contractor Risk Management) were combined with system-level Risk Management at the ESRT to develop a comprehensive, consistent Risk Management process that became routinely operational.

The central purpose of this report is to provide a knowledge asset repository for the National Reconnaissance Office that can be leveraged in support of further Risk Management efforts.

1 Introduction

1.1 Letter from the IDP Program Director

The IMINT Development Programs (IDP) Risk Management effort began as a result of the National Reconnaissance Office's growing recognition at the management level that we were encountering a composite of new challenges.

In the past, the NRO was able to manage risk events through extensions of schedule and increases in financial resources. In addition, all programs and operations were internal, and capable of being managed by the NRO alone. Now, the organization has necessarily changed the way we do business.

> *Risk Management forums 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."*

The global environment is changing to a world of more complex and rapid security needs. Technical programs are increasing in innovation, complexity, and sophistication. The divesting of system responsibility to mission partners requires a higher level of cooperation and a meshing of divergent program operations. Customer requirements are more complex and distributed. As a result, there is a much higher need for the Imagery Intelligence (IMINT) Systems Acquisition and Operations Directorate to be proactive, to have early visibility into risks, and to structure effective mitigation strategies to leverage reduction and management of these risks.

We were working to deliver mission-critical systems with new levels of visibility and new constraints in schedule and budget. Risk Management provides an ability to marshal financial, technical, management, and human resources to achieve program goals. It was clear that, without a system Risk Management process, the program was likely to encounter unforeseen, unplanned, and costly delays and obstacles.

Even though the needs were clear, rollout and installation of Risk Management required planning. Accomplishment of a government system Risk Management process required some significant culture changes. There was a legacy, based on long-standing experience, that funding and schedule, if not limitless, were readily accessed. As a result, there was widespread management disbelief that government Risk Management was necessary, or would be an asset. The culture was one in which both leaders and contributors were ready to focus on risks "when we get there."

In addition, because of technical contract requirements, segment contractors had incorporated at least some level of Risk Management. However, a government Risk Management process was not in place. The mission focus of government Risk Management was largely missing. Furthermore, government/contractor partnerships to address risks jointly were virtually non-existent.

We wanted to establish an effective Risk Management culture in which everyone in the system accepts accountability to anticipate risks—where the awareness of risks was adopted across all programs. Our goal 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 in which 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."

At IDP, to integrate the strongest possible Risk Management into our program, we decided to install system Risk Management through a developmental process. The first step was the pilot program at Seg 4. Once that process had proved itself, we installed Risk Management at the system level, to lead the way for the rest of IDP. Next, each division underwent training in Risk Management processes and practices, which helped us to develop a common language and set of tools to use across the system.

As a result, we were able to establish communication between segments and program concerns. System Risk Management allowed IDP, for the first time, to analyze and work together on interdependencies at the system level. Through the division Risk Management processes and the EIS System Risk Management Team, a consistent system Risk Management process was installed. The divisions found themselves increasingly able to communicate to their contractors' mission-critical Risk Management concerns.

A seldom-discussed but very real return on investment for Risk Management is that the process lays the groundwork for real management team building. The system Risk Management team meetings provide one of the few forums where people can talk openly in a non-status and non-threatening manner. This kind of open discussion builds a stronger management team. In these forums, there is no discrepant goal except to achieve real Risk Management. The discussion is not about segment success or failure. Participants are not required to present a "strong face"; each can request and receive assistance from others.

The Risk Management forum is 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."

Of course, the Risk Management process can only be as successful as the senior leader and his or her managers are receptive to learning about risks.

Our experience showed us that establishment of a successful Risk Management process requires some effort and planning. The essential elements we discovered are the following:

1. Start early. Risk Management is most effective when built into the system up front. If the process begins later, the change is more difficult. Whenever Risk Management is launched, culture change is required; this will slow the initial process but will accelerate program progress in the long run.
2. Roles in the process should be well defined and well understood.
3. Management must communicate clearly that roles for individual contributors and their managers are *different*—equally important, but even in an "open communication" culture, the chain of command and decision-making authority still resides in the hands of the managers. Contributors are valued but take their appropriate role in the management chain.
4. Make sure that there is a consistent set of tools—software tools, forms, formats, etc. Because divisions were initially operating rather autonomously, there was difficulty in the "flow-down." Think through how to install system Risk Management both horizontally and vertically in the system.
5. While core standardization is helpful, whatever version of Risk Management is rolled out must be tailored by each organization in which it is installed—each organization must set the process in place but then refine it to fit their needs. "Don't leave your common sense at home." Be aware of the pitfall of over-standardization and make sure Risk Management meets the needs of the program and the organization.
6. Management commitment is invaluable, and this must flow down all the way through the segments. Managers cannot assign Risk Management leadership to individual contributors; Risk Management will not be taken seriously without appropriate and visible leadership. IDP segments would not have had their successes if their division chiefs had not been present and actively engaged in their Risk Management efforts. Managers must become knowledgeable along with their people, and maintain continuous involvement in the progress of Risk Management. Even at the system level, delegation can only be to a senior person who can give direction and have it followed—as was the case, for instance, with the IDP deputy director who chaired the ESRT. Risk Management is only as good as the dedication of time by program leaders.
7. A proposed next step for the development of Risk Management, research into coupling Risk Management and earned value, may reap rewards and merits investigation.

In a very real sense, just as Seg 4 was the pilot for Risk Management for IDP, IDP was a pilot for IMINT as a system organization tackling rollout and installation of a government Risk Management process. While there were lessons learned at IDP that can be leveraged for IMINT and NRO Risk Management installations in the future, there were some conclusive solid successes. As with any process, further gains can be achieved through further maturation. Still, our essential goals for Risk Management—early warning of potential risks, cost savings, schedule alignment, effective management of margin, and reduction in negative surprises—achieved significant gains at IDP.

The most important recommendation for the future is this: Risk Management is not a "fad *du jour*"—it is one of the most powerful management methodologies developed so far. Risk Management is essential for program security and success. Risks need to be incorporated into the defining of a program critical path. Resources spent for risk mitigation, when targeted to the right risks at the right levels, are more than cost-effective. The return on investment includes a proactive, strategically focused, success-oriented program.

Al Krum
Director, Systems Engineering Sector,
IMINT, NRO
(formerly Program Director, EIS)

1.2 Purpose of This Report

This technical report is provided at the request of IMINT leadership to assure a written record of rollout and installation of Risk Management at IMINT during the two-year period from 1997–99. In response to this request, the report has been designed to address three interlocking goals:

- to describe the linkages between the key business needs and goals at IMINT that led senior leadership to initiate Risk Management
- to provide a conceptual framework of some best practices and process guidance in Risk Management that will facilitate further maturation and dissemination of IMINT Risk Management across IMINT
- to tell the story of actual experiences drawn from the rollout and installation of Risk Management at IMINT, tailored and shaped by the organization and its contractors to align Risk Management as a process that provides a critical factor in program success, as well as to identify success stories and lessons learned to enrich and accelerate future Risk Management efforts across the organization

1.3 A Map to the Report

The report is organized to provide insight and valuable knowledge regarding the three goals listed above. In addition to the report itself, certain key products of the Risk Management efforts at IMINT are provided in the Appendices to further identify the specific events, processes, and interrelationships developed at the EIS system level and throughout divisional Risk Management practice.

The sections of the report are as follows:

- **1 Introduction**

This section outlines the purpose and goals for the report, and describes the contents and their potential applicability for IMINT.

- **2 History and Background**

This section describes the establishment of the working relationship between the NRO and the providers of expert support from the SEI in the development of the IMINT Risk Management process. It includes a description of the original SA-CMM assessment and an explanation of the rationale for the selection of Risk Management as a cornerstone for acquisition improvement at IMINT.

- **3 Risk Management: Core Processes, Core Results**

This section provides a conceptual framework and high-level guidance for Risk Management process and practice. The reader should come away from this section with insight into the overall practice of Risk Management that will actually contribute to program success. For

those less familiar with the two-year history of rollout and installation of Risk Management at IMINT, this section will leverage a better understanding of the goals and methodologies that guided specific activities in the divisions and at the system level.

The section concludes with a "bridge" section on culture, change management, and sponsorship, which outlines the critical importance of the context in which Risk Management is necessarily embedded, and the success factors intrinsic to rollout and installation of system Risk Management at IMINT.

- **4 IMINT Goals for Risk Management**

This section provides information on critical program goals and other business needs on which Risk Management was focused. IMINT goals provide the essential results expected from Risk Management to support successful programs.

- **5 Rollout, Installation, and Infrastructure**

This section contains descriptions of the rollout and installation of Risk Management as it was practiced in divisions and at the system level at IDP/IMINT, including examples of tailoring that are unique to each division. This section also describes the standardization at the system level required to achieve cross-organizational program alignment and reap benefits from the IMINT goals for Risk Management.

Actual experiences of Risk Management at IMINT are also presented, outlined in rough chronological order. Section 5.1 describes the experiences of Seg 4, the original pilot division.

Section 5.2 describes the creation of the pivotal Risk Management Tool; later, section 5.3.5 describes the adoption of the tool as the system standard. Section 5.3 describes the establishment of the system-level Risk Management team.

Section 5.4 contains the actual experiences of divisions in their Risk Management rollout and installation; 5.4.1 defines the key success factors, investments, rollout plan, and implications that can be drawn for future installation. Section 5.4.2, a section that owes a special debt to generous interviews with actual NRO managers and technical staff, describes in a lower level of detail those occurrences that proved important to each division in its rollout experience.

- **6 Knowledge Management: Success Stories, Lessons Learned, Recommendations**

This section is especially important for leveraging business results from Risk Management from established Risk Management processes.

The knowledge management information in Section 6 is provided to leverage data and information that will be useful for the future of Risk Management at IMINT and elsewhere. It

identifies contributions from actual divisional Risk Management experiences for continuing development.

- **Appendix**

The appendix is intended to provide a rich repository of actual tools, plans, and techniques, as well as articles, guidance, and suggestions for improvement.

2 History and Background

The Risk Management effort at IMINT actually began in 1995, when NRO executive leaders were seeking ways to modernize and improve NRO operational capability. As discussed in the preface and the introduction, there was widespread recognition of NRO technological leadership. However, NRO leaders decided that the organization's ability to continue their heritage of excellence would require new levels of rigor in operational capability. This understanding led to a fresh look at best practices and outreach to obtain support in evolving those practices as inherent NRO capabilities.

Consequently, in winter 1995, NRO leaders attended the Software Engineering Institute Visitor's Day to obtain a fuller understanding of the range of SEI capabilities (see Figure 8, Overall IDP Risk Management Rollout and Installation Events Map). This interest of NRO leaders derived from their awareness of SEI as a DoD-sponsored federally funded research and development center (FFRDC), committed to support for organizations in maturing their internal engineering practices and management.

The NRO/SEI relationship has developed into a strategic partnership, dedicated to providing mutual benefit and to enhance opportunities of success for the large, complex systems that the NRO is required to produce and maintain in the national interest. Based on their joint understanding that lasting improvement occurs incrementally, the NRO/SEI relationship was designed as a collaborative one. The SEI was committed to assisting the NRO—and specifically, to begin with, IMINT—to achieve their mission-critical goals and objectives. SEI benefited from the opportunity to improve technology transition processes. The collaboration ultimately was founded on a joint commitment to provide practical, effective software practices to DoD, government, and industry.

As the initial collaborative effort, rollout and installation of Risk Management (based on the Software Acquisition Capability Maturity Model (SA-CMM) Level 3 Key Process Area, Acquisition Risk Management) was determined to be the optimal approach for providing immediate strategic and tactical support to IMINT executives, managers, and technical specialists. It was determined that this approach would mitigate preventable problems throughout program life cycles, and develop effective capability to surface and address risks in a constructive manner.

2.1 Software Engineering Institute

The mission of the Software Engineering Institute (SEI) is to provide leadership in advancing the state-of-the-art practice of software engineering to improve the quality of systems that

depend on software. To this end the SEI has been working with government and industry software acquirers and developers to improve the current software engineering practice in their organizations. To effect these improvements, the SEI uses a structured and integrated transition approach for systematically introducing technology into an organization and maturing its use to acceptance as standard practice. In this sense, technology refers to any process, methodology, tool, or technical solution that improves the ability to develop and maintain software systems. The goal of the SEI approach, when working with an acquisition organization, is to improve the quality of the organization's software products. The SEI achieves this by assisting in improving its software acquisition process, in working more effectively with its software contractors, and in the application of technical software solutions to the acquisition and maintenance of its software intensive systems.

2.2 The National Reconnaissance Office

The National Reconnaissance Office (NRO) designs, builds, and operates reconnaissance satellites for the United States of America. NRO products, provided to an expanding list of customers, such as the U.S. Central Intelligence Agency (CIA) and the U.S. Department of Defense (DoD), can warn of potential trouble spots around the world, help plan military operations, and monitor the environment. As part of the 13-member U.S. intelligence community, the NRO plays a primary role in achieving information superiority for the U.S. government and armed forces. In 1993-94, the NRO underwent consolidation and relocation to its current East Coast offices. Staffed by DoD and CIA personnel, the NRO is funded through the National Reconnaissance Program, part of the National Foreign Intelligence Program.

As the 21st century approaches, the NRO is guided by its vision of being "Freedom's Sentinel in Space: One Team, Revolutionizing Global Reconnaissance." The mission of the National Reconnaissance Office is to enable U.S. global information superiority, during peace and through war. The NRO is responsible for the unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems and related intelligence activities needed to support global information superiority.

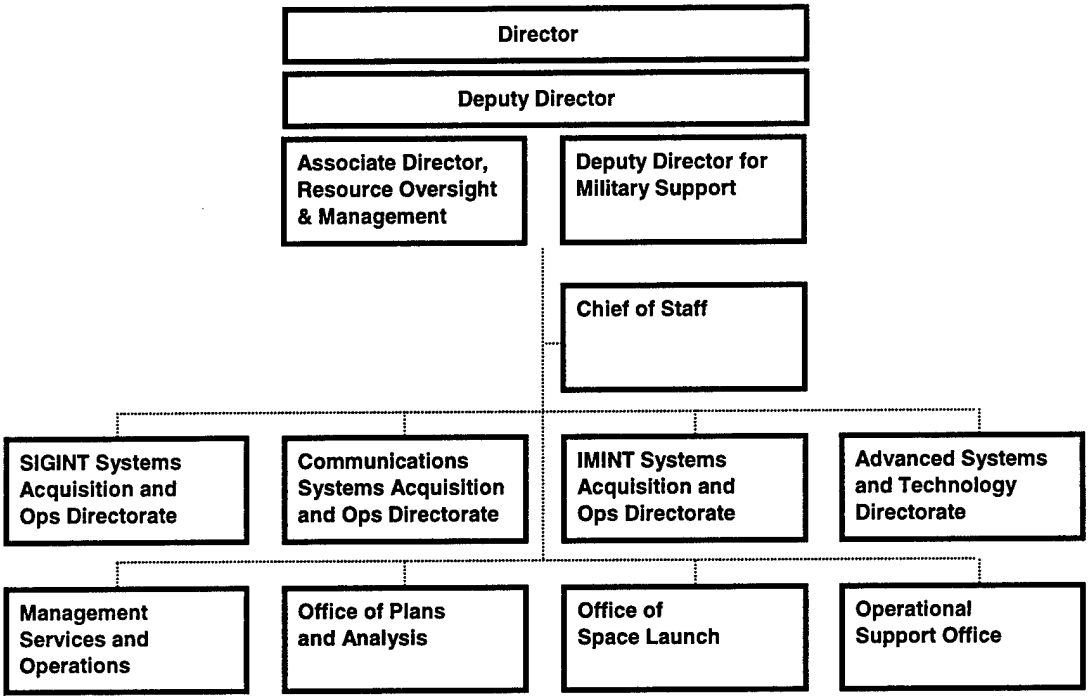
The NRO's Imagery Intelligence (IMINT) Systems Acquisition and Operations Directorate is responsible for the development and operation of imagery satellites that serve the National Command Authority, the Intelligence Community, and the military forces of the United States. Specific directorate functions include the development of reconnaissance technology for new systems capabilities, the acquisition of spacecraft and supporting ground-based systems, and the management of the day-to-day operations related to imagery collection, processing, production, and distribution.

The IMINT Enhanced Imagery Systems Division (IMINT/EIS) is responsible for the development of several large and complex systems that involve the incorporation of millions of lines of software. These systems cover a wide variety of technical disciplines and applications and involve a diverse set of users, both highly technical and non-technical. The devel-

opment methodology employed by IMINT/EIS has evolved over 20 years and is documented in a program office directive (the IMINT Standard for Program Development, IMSPD) and a Configuration Management Plan (CMP). The IMSPD and the CMP are used by the community of NRO contractors and the program office technical monitors in development of the various elements of the systems. Development efforts are generally multi-year, software intensive, and include extensive design documentation—and are therefore costly.

The following chart shows the organization of the NRO:

Figure 1: National Reconnaissance Office Organization Chart



2.3 Decision to Pursue Risk Management

In deciding to focus initial improvement efforts on Risk Management, IMINT leadership based their decision on the underlying assumption of IMINT acquisition strategies—that significant savings and technical reliability for mission-critical systems would be achieved by advances in acquisition excellence. Decision makers sought to increase the NRO's ability to promote success of program development, delivery, operations, and sustainment through forecasting and management of risks. Life cycle development costs and schedules for new systems, as well as system performance issues, were to be considered early in the design process. Sustainment and logistics for existing systems needed to be addressed through process improvements and best practices in technology insertion capability. Critical system interfaces between components and between lifecycle phases were to garner newly focused attention. These goals were formulated in the context of rapid delivery and high performance demands.

As a result, the collaborative effort between NRO and SEI began with a long-term intention to further develop system capability through a broad range of best acquisition and management practices. There was also a decision to discover the current and optimum levels of performance by IMINT. Therefore, the organization decided to conduct a Sofware Capability Maturity Model assessment to determine the current state of acquisition practice. Once these findings were obtained, with an array of potential improvements, IMINT leadership decided

to prioritize its first efforts on Risk Management, in order to leverage broad, relatively accelerated results and return on investment.

2.3.1 Software Acquisition Capability Maturity Model Assessment Findings

Originally, the IMINT directorates contracted with the SEI in March 1996 to provide guidance in Software Acquisition Capability Maturity Model (SA-CMM) Internal Process Improvement. An assessment using the SA-CMM at IMINT was conducted in August 1996 by a joint NRO/SEI/Aerospace team led by Larry C. Jones. The objective of the SA-CMM assessment was to focus on improvement opportunities for IMINT in its ability to acquire, develop, and deliver—in less time and with reduced life-cycle costs—highly reliable systems that meet the needs of the IMINT customer community.

The SA-CMM, a five-staged maturity model for acquisition process improvement, has 17 key process areas (KPAs) spread across Levels 2 through 5. For the IMINT assessment, all key process areas in Level 2 were assessed, as were four of the five key process areas at Level 3. The assessment found significant program strengths at IMINT as well as important improvement opportunities. The assessment yielded 25 recommendations for improvement. The SA-CMM model contains Acquisition Risk Management as a Level 3 key process area. In addition, the SA-CMM model has implications for risk, quality, productivity, and rework that can be seen graphically in the following chart:

Table 1: SA-CMM Key Process Areas

Level	Focus	Key Process Areas	
5 Optimizing	*Continuous process improvement*	Acquisition Innovation Management Continuous Process Improvement	**Higher quality and productivity, lower risk**
4 Quantitative	*Quantitative management*	Quantitative Acquisition Management Quantitative Process Management	
3 Defined	*Process standardization*	Training Program Acquisition Risk Management Contract Performance Management Project Performance Management Process Definition and Maintenance	
2 Repeatable	*Basic project management*	Transition to Support Evaluation Contract Tracking and Oversight Project Management Requirements Development and Management Solicitation Software Acquisition Planning	**Higher risk, rework**
1 Initial	*Competent people and heroics*		

2.3.2 Selection of Acquisition Risk Management as the Initial Improvement Initiative

The gap in program management practice meant that, according to the SA-CMM report:

> *Without a systematic risk identification program, IMINT is subject to the untimely discovery of problems that include poor performance as well as cost and schedule overruns. Furthermore, without the benefit of risk information, programmatic decisions may not have all the necessary information. Ultimately, the lack of risk information has the potential for IMINT to set inappropriate program priorities.*

The original intention of the SA-CMM assessment was to provide a platform for software acquisition process improvement. However, upon consideration of the overall SA-CMM findings, and after discussions with SEI representatives and the joint NRO/SEI team members, IMINT leadership decided it could achieve optimum near-term results by focusing efforts first on acquisition Risk Management.

The initial strategy to enact effective acquisition process management, therefore, was to initiate both short-term and comprehensive Risk Management programs. The short-term strategy included

- establishment of sponsorship for the effort by the management team
- a pilot program to define government-level Risk Management
- a system-level Risk Management program

The longer-term, comprehensive strategy included

- creation of a transition plan for how to manage rollout of Risk Management from the pilot across other IMINT divisions
- solicitation of input from across the organization on best installation strategies
- establishment of plans to establish collaborative and consistent processes by contractors and government, including training to roll out the practice across IMINT

2.3.3 Additional Drivers for Acquisition Risk Management in New Factors Impacting the NRO

Expectations for Risk Management by IMINT leadership included the promise of enhanced communications, especially between the government and contractors. The new context affecting the NRO—including increased congressional scrutiny, government-wide budget cutbacks, greater pressure for first-time program success, and the need to strengthen the corporate culture to support success—led IMINT senior management to select Risk Management as a critical initiative. Risk Management practices tend to support open dialogue that is vitalized by multiple perspectives on technical, business, and performance concerns.

An additional dynamic affecting all of the NRO was the increased openness of the intelligence community. More information about NRO operations was being made available to congress and the public, which was in itself a culture shock for the organization.

A related factor driving the NRO to optimize resources, set the best possible management and program priorities, prevent problems from occurring, and proactively identify and mitigate risks is a government environment of reduced budgets and increased Congressional scrutiny on program costs and operations.

2.4 Technology Forum

In an effort to focus widespread attention at the NRO on potential opportunities that can be afforded by improvements, IMINT leaders decided to hold a joint NRO/SEI Technology Forum, which was held in July 1997. Keynote remarks were made by Brigadier General Robert E. Larned, with presentations made by the SEI technical and management practices programs. The forum was designed to provide for interactive exchange, and therefore small groups met to allow for discussion of questions and issues of interest to the NRO.

This Technology Forum led to a range of collaborative events and relationships between the NRO and the SEI, including a series of presentations by the NRO Acquisition Center of Excellence on the Sofware Acquisition Capability Maturity Model, and parallel SEI initiatives to the Risk Management effort. The interest generated in continuing open dialogue between the NRO and the SEI has established subsequent forums, communications, and participation by NRO leaders at a number of SEI conferences, including the annual Software Engineering Institute Symposium.

The commitment across the NRO, and in particular at IMINT, continues to be expressed in mutual efforts to attain the NRO's strategic goals and missions.

3 Risk Management: Core Processes, Core Results

3.1 The SEI Risk Management Paradigm and IMINT Risk Management

The following is the Webster's Dictionary definition of *risk*: "Risk is the possibility of suffering loss." There are two underlying elements that help explain this definition:

1. *possibility*: an event that has not yet happened, but is at least likely
2. *loss*: unwanted negative consequences or adverse effects

Risk Management, then, addresses future uncertainty and partially unknown events that have a likelihood of serious negative impact. Addressing risks requires the communication of two unpopular considerations: bad news and uncertain possibilities.

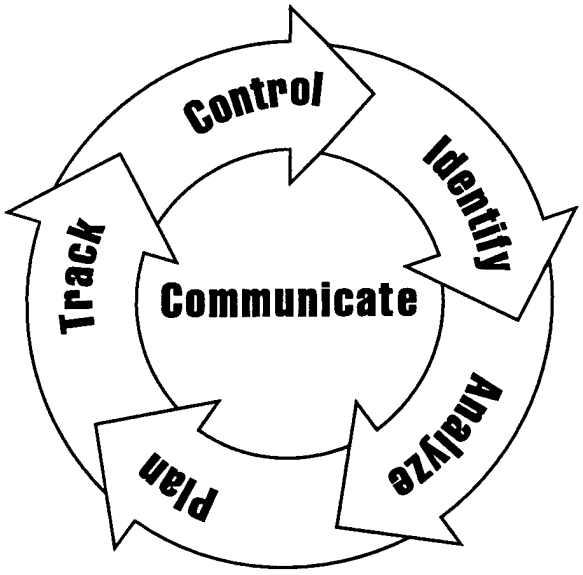
Therefore, a successful rollout and installation of Risk Management in *any* organization requires cultural, management, and infrastructure preparation. It also requires an acceptance, sponsored by organizational leadership, that Risk Management is not a one-time process. Indeed, Risk Management is really a "knowledge management"[1] approach to program management. That is, Risk Management encourages proactive identification of probable but as-yet unrealized events, and further promotes the transformation of isolated data points into compiled and useable information. Then, through the emphasis on multiple perspectives, Risk Management supports organizations in leveraging information held by individuals into integrated knowledge that can be used by the entire organization. The rollout and installation at IMINT took advantage of the range of SEI methodologies, including training, tailoring Risk Management practices to fit each unit, establishment of a Risk Management infrastructure, and technical consultation to create a solid foundation for durable Risk Management.

IMINT established a disciplined environment for proactive, continuous Risk Management. Each division installed some form of Risk Management, tailored to that division's technical and program priorities and ways of doing business. Increasingly, IMINT divisional leadership and staff recognized the importance of *government* as well as contractor Risk Management. With system-level leadership, IMINT reached a level of engagement in continuous Risk Management that exemplified the Risk Management paradigm to

[1] For a further discussion of knowledge management, see chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

- *identify* new risks periodically to incorporate events from evolving project life cycle stages and other system and intersystem changes
- *analyze,* prioritize, and re-prioritize risks when appropriate to determine the priority risks to manage
- *plan,* decide best courses of action, and implement pertinent mitigation strategies to address priority risks
- *track* risks on a regular basis, integrated into overall program management
- *control* risks under consideration, making decisions on replanning and newly identified risks as part of the continuous Risk Management cycle
- *communicate*, throughout the process and throughout the organization, with open discussion to assure early identification of risks and full proactive exploration of best approaches to manage the risks

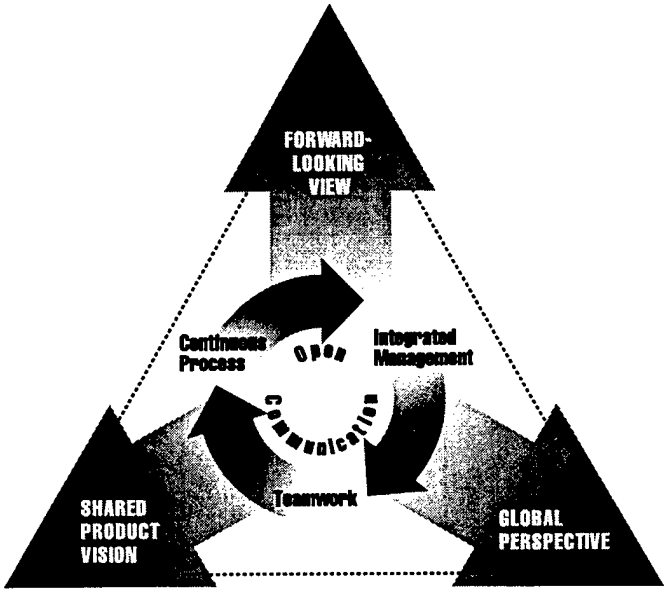
Figure 2: Risk Management Paradigm



3.2 Principles of Risk Management

Risk Management as defined by the SEI Risk Management paradigm is, in fact, a Continuous Risk Management (CRM) process. Results are achieved over time. New risks are identified, existing risk mitigation plans evolve, and risks are found to have dependencies. The organization profits from the examination of tradeoffs among alternative courses of action. Fundamental to this process is effective communication.

Figure 3: Principles of Risk Management



The core principles of Risk Management could be described as the "critical path" for Risk Management to provide support for successful programs. These principles provide guidelines that can be used to explore whether a system has the "right stuff" to leverage Risk Management to achieve program improvement.

The principles include three major components:

1. *the core principle*: open communication
2. *the sustaining principles*: integrated management, teamwork, and a continuous process
3. *the defining principles*: a forward-looking view, a global perspective, and shared product vision

Specific descriptions of each of these principles follow.

3.2.1 Core Principle: Open Communication

The purpose of this principle is to encourage the free flow of information at all project levels and between them. This enables formal, informal, and impromptu communication. Open communication is accomplished by using consensus-based processes that value individual (as well as the team's) input. This ensures that the system will benefit by bringing unique knowledge and insight to identify and manage risk.

3.2.2 Sustaining Principles

These principles are essential to maintain Risk Management and reinforce rollout and installation as a durable, established way of doing business in the organization. The principles emphasize the necessary integration of project management and Risk Management, cross-divisional and government/contractor cooperation, and ongoing attention. These principles include:

- *integrated management*. The underlying purpose of this principle is to help make Risk Management an integral and vital part of project management. This is accomplished by adapting Risk Management methods and tools to a project's infrastructure and culture.
- *teamwork*. The purpose of this principle is to create an environment in which individuals and teams work cooperatively to achieve a common goal by pooling talent, skills, and knowledge.
- *continuous process*. The purpose of this principle is to help a project sustain constant vigilance. This requires identification and management of risks routinely throughout all phases of the project's life.

3.2.3 Defining Principles

These principles define the critical ingredients for successful Risk Management. These principles access the best ideas, knowledge, and information assets of a system and include:

- *forward-looking view*. The purpose of this principle is to help the project team think toward tomorrow, identify uncertainties, and anticipate potential outcomes. The theme is proactive behavior: manage project resources and activities, while anticipating uncertainties.
- *global perspective*. The purpose of this principle is to help the project within the context of the larger systems-level definition, design, and development by recognizing both the potential value of the opportunity and the potential impact of adverse effects.

3.3 Functions of Risk Management

As discussed in this report and throughout Risk Management training and practice, communication is at the hub of successful Risk Management. However, "communication" covers a very large territory, and in the case of Risk Management, some very specific skill sets are associated with each function. These capabilities must mature alongside any effective rollout and installation process.

In a system such as IMINT, where a Risk Management Tool has been designed and tailored for use both by divisions and by the overall program management, the tool itself will require an underlying competence in the Risk Management knowledge base, the right communications skill sets for sound knowledge management, and a system-wide Risk Management process to leverage successful results.

Below are the specific functions—identify, analyze, plan, track, and control of risks—and required activities for the Risk Management process, together with the related communications that will achieve results for each function.

Table 2: The Functions of Risk Management

Function and Its Purpose	Description	Communication Skill Sets for Each Function
Identify Search for and locate new or emerging risks before they become problems; define risk statements and context with basic risk data.	identify new risks risks are described in risk statements that include the *risk condition*, plus the *risk consequence* the *context* of risks is clarified	everybody identifies risks staff overcomes "fear of the boss" in bringing up sometimes uncomfortable news "the boss" overcomes fears of loss of control—rewards rather than kills the messengers everyone begins to practice "Risk Management culture"—the ability to accept a level of unpredictability and "bad news" together with candid and open team/project dialogue on risks
Analyze Transform risk data into decision information; define what is important to the project; set Risk Management priorities.	define *attribute criteria: impact, probability, timeframe* *classify* risks to group, consolidate, and enhance decision making *prioritize* risks to determine which will receive the most focused attention	team brainstorming, openness to thinking "outside the box" competence in management of opposite views capability to handle surprises, less desirable consequences strategic as well as tactical focus consensus management
Plan Translate decision information into decisions—establish mitigation plans and other options to handle risks; implement mitigation plans.	decide which of four approaches to take with priority risks: 1. watch 2. accept 3. research 4. mitigate (either a simple action plan or fully articulated mitigation plan) decide risk "owner" (whether to *keep, delegate*, or *transfer* ownership) develop *measures* to track mitigation plan progress	discuss/design options for alternate scenarios criteria definition as basis for decisions selection against criteria communications strategy and discipline to capture and present plans to senior management with clear information and clear requests for resourcing, etc. development of simple, targeted, relevant measures that motivate rather than disincentive systemwide Risk Management facility in relinquishing narrow interests to focus on success of the entire program and weigh interface impacts
Track Monitor progress of mitigation plans; programs collect measures and track risk indicators.	*acquire, compile*, and *report* data indicators for triggers, thresholds, and contingency plans periodically assess risk status	capitalize on consistent, visible management sponsorship to build buy-in across the program for Risk Management mechanisms to preserve confidenti-

		ality as well as timely open communications, as needed refined capability in graphic/visual communications for understandable presentations on risks and mitigation strategy updates agreement on standardized forms for optimum clarity in presentations on risk translation/dialogue across projects to leverage system-integrated mitigation plans mechanisms to resolve genuine conflicts capitalize on facility to focus on entire program success to resolve full-program impacts and improve decision quality
Control	decision makers *analyze, decide,* and *execute* based on status as appropriate (e.g., execute mitigation plan, replan, close a risk, invoke contingency plan, continue current actions)	management ability to elicit the best information from projects, especially with regard to vulnerabilities presentation and use of management-relevant measures by projects management regularly provides timely, candid guidance on program goals, priorities, and milestones used for their decisions mechanisms to shift larger issues further up the chain to next level of senior management, accompanied by clear, concise, and candid information for their decisions readiness to redesign mitigation/contingency plans when progress has been weighed and new directions are appropriate and management-relevant

3.4 Increased Pressure for System Risk Management from Official Mandates and Actions

In May 1999, the second edition of the *Risk Management Guide for DoD Acquisition* was issued by a consortium of the DoD Test, Systems Engineering and Evaluation, Defense Acquisition University, and Defense Systems Management College <URL: http://www.dsmc.dsm.mil/pubs/gdbks/risk>. This pivotal guidance document introduces the practice of Risk Management by stating:

> *Risk has always been a concern in the acquisition of Department of Defense (DoD) systems. ... [S]ome Program Managers ... viewed risk as something to be avoided. ... This attitude has changed. DoD managers recognize that risk is*

inherent in any program and that it is necessary to analyze future program events to identify potential risks and take measures to handle them.

The DoD risk management concept is based on the principles that risk management should be forward-looking, structured, informative, and continuous. The key to successful risk management is early planning and aggressive execution.

Furthermore, while IDP began its Risk Management in the software-development organization, the expansion of Risk Management across the system is clearly supported by the DoD mandate that "effective risk management requires involvement of the entire program team. ... [T]he risk management process should cover hardware, software, the human element, and integration issues."

There is a growing recognition of the importance of Risk Management in all government organizations, and the DoD has underscored this priority with several key DoD documents:

- The Fiscal Year 1996 Defense Authorization Act directs that " ... the process for acquisition of information technology is a simplified, clear, and understandable process that specifically addresses the management of risk, incremental acquisitions, and the need to incorporate commercial information technology in a timely manner."
- DoD Directive 5000.1, "Defense Acquisition" (March 15, 1996) provides for a " ... streamlined management process that emphasizes Risk Management and affordability ... [and] that explicitly links milestone decisions to demonstrated accomplishments."
- The DoD Defense Acquisition Deskbook includes a compendium of acquisition-related guidance, both mandatory and discretionary, including guidance on Risk Management <URL: http://www.deskbook.osd.mil>.

3.5 Investments Required for Risk Management

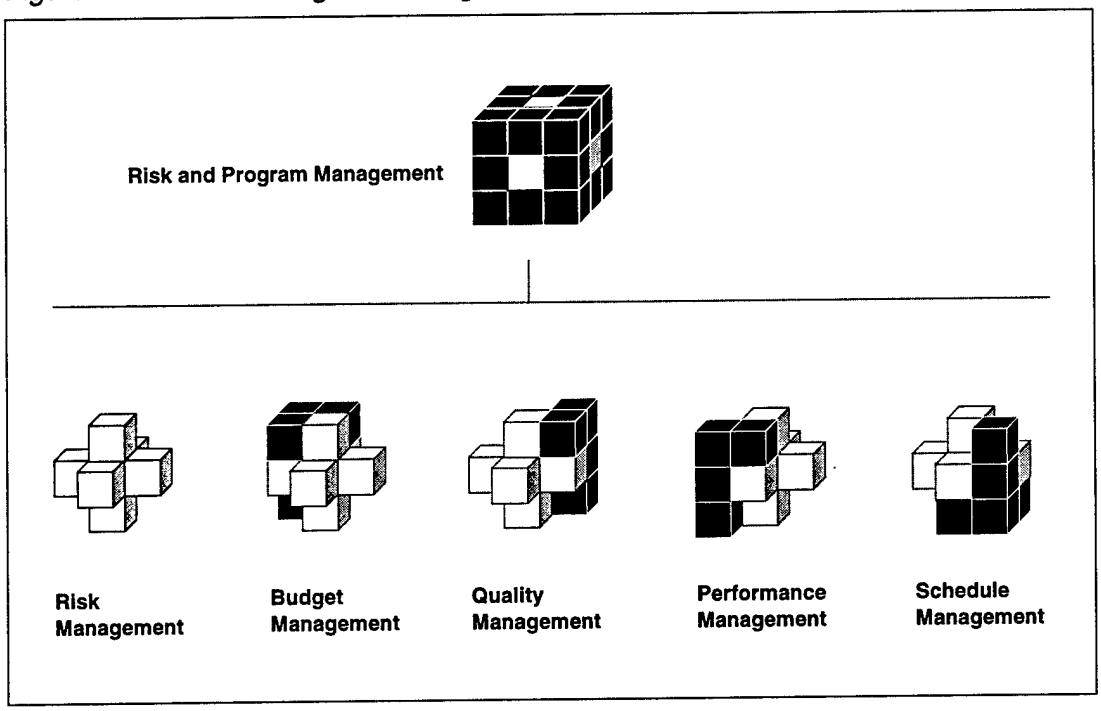
Organizational members correctly perceive that there are investments to be made in Risk Management, in terms of both time and other resources. Time investments include:

- staff time as a team for knowledge transfer (through training and process definition and installation activities)
- staff time for team dialogue and decision-making on risk identification, analysis, mitigation planning, and tracking
- time invested by some members on development and data entry to document risks and their progress
- time for government/contractor coordination on joint risk management, as well as government oversight of contractor Risk Management. Whether these take place through a regular Team Risk Review, as occurred in Seg 4, or through more informal coaching and communication to align processes and joint government/contractor risks, as occurred in Segs 32 and 2, there is measurable time required.

In addition to time investments, the following cost investments are subtle but nevertheless real:

- negotiations with contractors, which often must take place when a contract is underway and Risk Management is installed during the course of the contract
- holding offsites, when desired, which entails logistical costs
- materials development, which can range from negligible to a serious organizational investment, such as the Risk Management Tool
- resourcing for ongoing Risk Management coordination, activities, continuous building of the knowledge base through training and other education, maintenance of the Risk Management data and repositories, etc.
- resource investments that are granted by senior management as a result of management reserves, and persuasive Risk Management mitigation plans that require funding

Figure 4: Risk and Program Management



3.5.1 The Interface Between Risk Management and Program Management

Under technical, political, and customer pressure to provide successful near-term program results, the natural temptation is to focus away from long-range, critical-path thinking and focus only on short-term results. Short-term focus itself then becomes a risk to program success—over the entire program life cycle, and for the ultimate success of program delivery.

As the *Risk Management Guide to DoD Acquisition* states:

Risk management should be integral to a program's overall management. [Program managers] must take an active role in the process to ensure that their approach leads to a balanced use of program resources, reflects their overall management philosophy, and includes government and contractors. Past DoD practices have generally treated risk management solely as a system engineering function, cost-estimating technique or possibly as an independent function.

Today, risk management is recognized as a vital integrated program management tool that cuts across the entire acquisition program, addressing and interrelating cost, schedule, and performance risks. The goal is to make everyone involved in a program aware that risk should be a consideration in the design, development, and fielding of a system. It should not be treated as someone else's responsibility.

As many organizations are discovering, whether or not to take risks is no longer a real option. Many government programs now involve such extensive requirements for innovative and groundbreaking technologies that risks are necessarily involved. Once Risk Management is integrated with program management to assure future-oriented identification, mitigation, and management of risks, reasonable risks can be taken, providing fresh opportunities for advancement that may not be visible before Risk Management is instituted.

As stated by Roger L. Van Scoy in *Software Development Risk: Opportunity, Not Problem* [Software Engineering Institute, CMU/SEI-92-TR-30 ADA 258743, September 1992]: "Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity."

For organizations installing Risk Management, full integration into system program management provides growing understanding, acceptance, and commitment across the organization—vertically and horizontally.

3.6 Establishing the Risk Baseline

There are multiple approaches to establishing a risk baseline in an organization: divisions/project teams can hold offsites to brainstorm and capture their portfolio of risks; projects can identify past performance risks that resulted in project slips, and utilize those to anticipate future risks; and a division can review its work breakdown structure and forecast those aspects where risks may reasonably be expected. The SEI has a number of approaches, including the Software Capability Evaluation (SCE), which is widely used to establish a baseline of risks from the perspective of the Software Capability Maturity Model. The SCE has been used elsewhere in the NRO to identify program and project risks.

A disciplined and proven effective approach was used for the IMINT Risk Management pilot program: the Software Risk Evaluation (SRE), which was developed by the SEI specifically

to focus on project risks. An SRE was conducted for both the government and the contractor of the pilot Risk Management program.

3.6.1 Software Risk Evaluation

The SRE is a diagnostic and decision-making tool that provides a robust, clear, and understandable picture of the risks that may affect a project. During an SRE, project team members can identify, analyze, create mitigation plans, and prepare to track and effectively communicate about risks in the development of software-intensive systems.

The picture that emerges may be used in a number of ways, including

- a pre-project diagnostic. Are the risks acceptable to start a project?
- a baseline. What are the critical project risks that have not yet become problems, and that need to be managed on a continuous basis?
- preparation for critical project milestones. What are the risks that need particular attention so that the project may remain on its critical path?
- crisis recovery. How can we reset the project baseline when re-plans are inevitable?

An SRE provides a structured, disciplined, comprehensive approach to identify and analyze both specific risks, and their interdependencies. The project's personnel participate in the identification, analysis, and mitigation of risks facing their project. Through the use of interviews based on a risk taxonomy, a full portfolio of project risks is identified.

A project may use an SRE at any time as a checklist to help make sure that multiple, major risks are forecasted and planned for proactively. An SRE provides a project manager and his or her staff with a structured, repeatable "early warning system" for anticipating and addressing project risks. The SRE further introduces a set of activities that begin the process of managing risks on a continuous basis. These activities can be integrated with existing methods and tools to enhance project-management practices.

Conducting an SRE has a number of benefits, including

- accelerating the development of a shared product/program vision among project staff
- providing a snapshot of risks
- creating a shared view and common framework for risks facing a project among the staff
- enabling the systematic tracking of risks and their mitigation plans by noting changes in probability and impact
- providing decision-making information directly to the project manager
- providing the impetus for focused project-level process improvement

In summary, the SRE approach provides the project not only with a method and artifacts that can be repeated and reused, but also with a process that can be institutionalized and readily adopted into the project's mainline project management.

A word of caution: to achieve the benefits from the SRE approach, the SRE needs an authorized, experienced leader and trained team members. In the absence of these safeguards, the SRE could yield faulty results and therefore adversely impact project members' ability to manage risks, which could harm project credibility.

3.7 Team Risk Management

The SEI has developed a process for government/contractor Risk Management called "Team Risk Management." This approach helps assure that the guiding Risk Management principles of *open communication, integrated management, teamwork,* and *shared product vision* are created for projects in an acquisition environment.

Team Risk Management is an approach allowing government and contractors to manage project risks together, based on their separate Risk Management processes, and their compiled list of top project risks.

Team Risk Management is a continuous practice performed by government/contractor teams, including, where appropriate, Integrated Product/Process Teams, who work during the lifetime of a project to effectively manage project risks. As with other approaches to Risk Management, a baseline set of risks is established first. Then the continuous activities begin. Risks are identified and analyzed in terms of their probability, impact, and timeframe. Risks are jointly analyzed to determine just which risks are most important, and to enable effective resource allocation. Mitigation plans are created to define and implement strategies to address the most important joint risks. Finally, risks and mitigation progress are reported to the joint team, so they may be tracked and controlled until the risks no longer exist.

In Team Risk Management, communication occurs at all levels and in all directions within the project to ensure that the right people have the right information that they need to make timely decisions, and to provide project team members with perspective on their concerns.

3.7.1 Team Risk Management Principles[2]

The cooperative approach to Risk Management has been very strongly endorsed by the DoD as well as government organizations. The most recent guidance on Integrated Product/Process

[2] This section contains some adaptations and excerpts from: *Team Risk Management: A New Model for Customer-Supplier Relationships,* by Ron Higuera, Audrey Dorofee, Julie A. Walker, and Ray C. Williams, July 1994; a presentation, *Team Risk Management: Expectations Setting Meeting,* by Rick Barbour for NRO, June 1997; *Risk Management in Accordance with DODD 5000 Series,* by Cpt. David L. Nordean, USN, Richard L. Murphy, SEI, Ronald P. Higuera, SEI, and Yacov Y. Haimes, Center for Risk Managment of Engineering Systems, University of Virginia, July 1997; and working documents between Jo Lee Loveland Link, Rick Barbour, and Richard L. Murphy, April 1998.

Teams (July 1998) from the Office of the Under Secretary of Defense (Acquisition and Technology) spells this out clearly. "Proactive Identification and Management of Risk" is one of five major IPPD "tenets" and stipulates:

> *[u]sing a multidisciplinary teamwork approach (wherein) designers, manufacturers, testers, and customers work together...DoD endorses a risk management concept that is forward-looking, structured, informative, and continuous. The key to successful risk management is early planning and aggressive execution.*

In addition, widespread government guidance now promotes government/contractor partnership in order to achieve the most effective program results, for example:

> *In an era of diminishing resources, partnering is a smart business strategy. The time that contracting officers and program managers invest in improving communication with their industry partners yields big dividends in better contract performance.*
>
> Gary A. Tull,
> Assistant Depty Chief of Staff for Research, Development & Acquisition, Army Materiel Command

> *Project risk management is the art and science of identifying, assessing, and responding to project risks throughout the life of a project and in the best interests of its objectives.*
>
> Project Management Institute
> Project Management Body of Knowledge

Furthermore, as described above, the SEI Software Acquisition Capability Maturity Model includes a Key Process Area (KPA) for Level 3 entitled Acquisition Risk Management. The KPA describes an organization in which project and program staff

> *identify risks as early as possible, adjust the acquisition strategy to manage those risks, and develop and implement a risk management process as an integral part of the acquisition organization's standard software acquisition process.*

The goals for the most recent version of the SA-CMM (Version 1.02) describe what is required to satisfy the KPA:

- Goal 1. Project-wide participation in the identification and mitigation or risks is encouraged and rewarded.
- Goal 2. The project team's defined software acquisition process provides for the identification, analysis, and mitigation of risks for all project functions.
- Goal 3. Project reviews include the status of identified risks.

In addition to the Acquisition Risk Management KPA, there is a KPA for Contract Performance Management, which includes the following:

- Goal 1. The quality of contractor team process...is appraised throughout the contractor's period of performance to identify risks and take action to mitigate those risks as early as possible.
- Goal 2. Contract Performance Management activities intended to foster a cooperative and productive environment among the end user, project team, and the contractor team are implemented.

For Contract Performance Management, Goal 3 (of 3) stipulates:

> *A cooperative and productive environment among the project team, the end user, and the contractor exists.*

In recent years, Acquisition Reform, the Information Technology Management Reform Act (ITMRA, also known as the "Clinger-Cohen Act"), and other legislation and initiatives have gravitated government operations increasingly toward being more performance-based and results-based to achieve successful program results. This higher level of performance expectations translates into a need for supplier/contractors to define technical design characteristics in a process in which two-way communication between government and contractor is mandatory.

Program and Risk Management practices that support effective communication, partnering, and teamwork will reduce the probability that misunderstandings will lead to major problems. Recognizing the importance of this trend for effective program and Risk Management, the SEI developed the Team Risk Management process to

- develop a shared product vision
- focus on results
- apply Risk Management principles and tools to cooperatively manage risks and opportunities

In keeping with the spirit of these initiatives and the government direction toward increased partnerships between the government and the contractor community, the SEI model of Team Risk Management provides a way for organizations to capitalize on partnership to achieve higher-level results. Team Risk Management is generally practiced either in sessions devoted

specifically to Risk Management, or in a set agenda time period for regular program-management meetings. Engaging both government and contractor in joint sessions, Team Risk Management builds on the separate Risk Management practices of both government and contractor.

Team Risk Management extends the Risk Management process to a Risk Management partnership between government and contractor. The formal definition of Team Risk Management is

> *an approach for customers and suppliers to manage risks and opportunities cooperatively and continuously using proven principles and tools of Risk Management.*

Risk Management, when performed in a "team" environment including government and contractor, reduces the risk of developing and delivering a system that will not meet the operational user's requirements. Team Risk Management creates opportunities for government, contractors, and users to identify perceived risks in development activities early, when more cost-effective corrections can be made, as well as throughout the program life cycle, as new risks emerge even as former risks are closed.

Team Risk Management principles include and amplify the principles of Risk Management. The following elements are supported by real-world examples from Team Risk Management at the NRO:

1. *shared product/program vision*: sharing a common purpose and ownership, committed to successful program delivery
   Example: While candidly discussing their different business drivers, one contractor provided information on the contractor's corporate planning, which was important input to a specific risk plan.
2. *teamwork*: while respecting appropriate confidential and proprietary concerns for both government and contractor, working in partnership to the common goal, integrating skills and knowledge
   Example: One contractor joined the government division for a "refresher" Risk Management training course, and revised its own Risk Management process to align more closely with the government's.
3. *global perspective*: operating from a systems context that includes up-the-chain management and mission partners, as well as internal divisional partners in program delivery
   Example: The contractor alerts its government customer to an interface risk between its system and that of another divisional system.
4. *forward-looking view*: anticipating downstream uncertainties or potential impacts or results from decisions made today
   Example: Both government and contractor in the ongoing Team Risk Review credit that forum for retaining their ability to have a "time out" for purposeful reflection on forward risks and to plan proactively for cost, schedule, and performance pay-offs.

5. *open communication*: establishing knowledge management as a core value, respecting diverse interests of government and contractor, building an atmosphere of candor, encouraging and capitalizing on different perspectives, working to forge agreements. More than ever, disclosure of risks needs to be rewarded, not blocked with disincentives.
   Example: In one Divisional System Review, the only "sharp words" between government and contractor came not when the contractor raised risks of an unexpected interface disconnect, but when a problem was raised that had not been heard as a risk.
6. *integrated management*: integrating program management and Risk Management to support the entire program life cyle through delivery
   Example: While taking care to differentiate between future risks and current issues, one contractor held "risks and issues" sessions to identify new risks and transfer issues to work when they are no longer risks but current realities.
7. *continuous process*: managing risks on an ongoing basis
   Example: One division has found a monthly Team Risk Review quite useful for a variety of reasons, including the regular reminder to "think in the risk context"; another uses regular project meetings to work on the government/contractor partnership.

3.7.2 Government/Contractor Partnership: The Heart of Team Risk Management

Team Risk Management provides a forum where government and contractor periodically review together risks, analyze and plan risks, and discuss parameters and potential tradeoffs. The result is to significantly improve joint communications, and shed light on risks that derive from government and contractor separately or together. Provided the TRM process is followed conscientiously and with candor, the project can achieve significant gains in reduced cycle time and product costs because of what one government manager refers to as "blunder avoidance."

Team Risk Management is based on principles that are very similar to the integrated product/process team model. As stated in the document, *DoD Integrated Process and Product Team Handbook*, " ... every member of the program team (government and industry) needs to work from the same information and toward the same overall program goals" <URL: http://www.acq.osd.mil/sa/se/ippd/ippd_pubs.html>. This approach is encouraged by the *Risk Management Guide for DoD Acquisition,* which states that

> *managing a program's risk requires a close partnership between the PMO and the prime contractor(s). ... The prime contractor's support and assistance is required even though the ultimate responsibility for risk management rests with the government PM. Often, the contractor is better equipped to understand the program technical risks than the government program office is. Both the government and the contractor need to share information, understand the risks, and develop and execute management efforts. The government must involve the contractor early on in program development, so that effective risk assessment and reduction can occur. ...Forming a joint government/contractor (risk management) evaluation team is a good way of fostering an effective partnership.*

Team Risk Management establishes a cooperative working environment throughout all levels of the program that gives everyone in the program the ability and motivation to look ahead and handle risks before they become problems. This is accomplished through regular interactions (usually monthly meetings, especially at first) and a practical set of practices, methods, and tools that join government and contractor together as a team to manage program risks.

Teamwork helps ensure that risks are cost-effectively managed throughout the program life cycle. Eventually, Team Risk Management becomes routine and continuous activities within the program can provide management at all levels of the system with information to make informed decisions on program-critical concerns.

Finally, while emphasizing joint management of risks by government and contractor, Team Risk Management restores the government to program accountability. Rather than having Risk Management conducted primarily (or even solely) by contractors, government managers and staff become knowledgeable about their own programs and the likelihood of success, well enough in advance to do something proactive and constructive, usually before risks become real problems.

One section chief has said, "The government model has been to pass the responsibility for Risk Management over to the industry partner, with little consequence if the Risk Management process failed. Programs were often over target costs and schedule. With current budget profiles, this approach is no longer acceptable. The new government Risk Management process places the government team in an accountable role for Risk Management and program results."

3.7.3 Benefits of Team Risk Management

The government/contractor partnership as practiced in Team Risk Management offers a number of advantages for a project/program, as compared to Risk Management practiced by individuals or government only. However, Team Risk Management also often involves evolution of past management practices and past government/contractor relationships, requiring new commitments by both. These new commitments in turn may entail investment—particularly early in the program.

The advantages and necessary commitments are described in the following table:

Table 3: Benefits of Team Risk Management

Advantage	Description	Required Commitment
Improved communications	This aspect of routine communications includes both customer and supplier. Risks are treated by all as depersonalized issues that threaten the common goal of a successful program.	Move beyond finger-pointing and resolve project risks as a joint responsibility. Encourage all forms of communication (e.g., telephone and electronic mail) among all team mem-

	By openly sharing risks, both the customer and supplier are able to draw on each other's resources in mitigating risks and enabling rapid response to developing risks or problems.	bers. Encourage all to explore what could cause the program to go off track. Allow for more meetings and more travel initially.
Multiple perspectives on risks	Team members are not limited to looking for mitigation strategies among their own limited areas of control. Bringing both customer and supplier together in mitigating risks opens doors to strategies that both can do together, but that neither could do alone.	Accept the philosophy that the team can arrive at better solutions than any individual—even the program manager—can alone.
Broader base of expertise	The combination of customer and supplier brings together a richer pool of experience in perceiving and dealing with risks. The customer often brings better perspectives on the application domain and "what's possible to change." The supplier often brings better perspectives on the technical domain and "what's possible to do."	Accept all the unique perspectives that others bring to the table.
Broad-based buy-in	Risks and mitigation strategies are cooperatively determined by the team (customer and supplier), so all accept the results of the process. "Second guessing" and criticism after the fact are eliminated. Over time trust develops and expectations are realized. This paves the way for strengthened relationships and the power of teamwork.	Encourage and allow teams to meet, discuss, and agree. Invest in improving meeting skills. Use outside facilitation as required.
Risk consolidation	Structured methods bring together risks identified in each organization, giving decision makers a more global perspective and highlighting areas of common interest and concern.	Accept that risk is inherent in enterprise. Abandon the notion that risks should not be discussed until a mitigation strategy has been identified.

[Higuera 94a]

3.7.4 Steps Toward Team Risk Management: Evolution is Workable

Since Team Risk Management builds on established Risk Management processes, it follows that Team Risk Management requires rather mature, established processes. Accordingly, the timing for installation of a robust Team Risk Management approach can vary considerably.

Closer government/contractor partnerships are very much encouraged as part of current acquisition legislation and as good contracting practice generally. However, when the stakes are high—for highly visible, politically sensitive, and innovative programs, for example—and the margin for error is low—new levels of budgets constraints, low tolerances for re-plans,

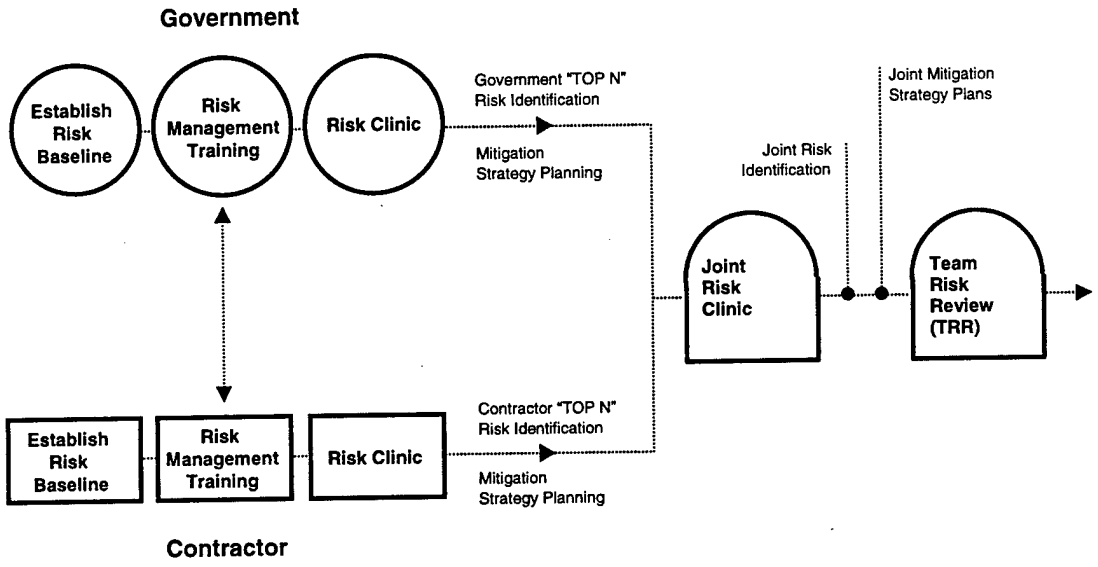
critical customer functionality needs, for example—solid and effective government/contractor partnerships can spell the difference between success and failure.

What may appear to be subtle, modest steps toward Team Risk Management may be precisely what is required for full development of a durable government/contractor partnership, and should not be dismissed as trivial.

3.7.5 The Evolution of Team Risk Management in a Program

The SEI model provides this general process flowchart for an organization committed to the practice of Risk Management:

Figure 5: Recommended Approach to Team Risk Management Installation



The three Risk Management activities identified vertically contain outcomes that can be achieved in more than one way, or for which timing is somewhat elective:

- *Establishing the risk baseline.* This is a critical first step. As described above, at IMINT the SRE was selected as the most disciplined and productive approach to capturing the repository of program risks by both government and contractor.

  The purpose of the SRE is risk identification, and alternative approaches are possible. However, for a project or system new to Risk Management, a full SRE can be a real asset.

- *Risk identification.* As indicated in the flowchart, risk identification for a division or systemwide may first occur *after* training and the Risk Clinic. Indeed, risk identification is not a one-time-only event, and even an organization that has undergone a full SRE/TRE will need to encourage ongoing risk identification.

As new risks emerge and are identified, older risks are successfully mitigated and may be closed or, for those risks that become issues despite mitigation, transferred for management as issues.

- *Mitigation strategy planning*. Mitigation strategy planning may be conducted at a number of points in the Risk Management process—after the initial SRE, following the Risk Clinic and the initial risk identification, during an initial Team Risk Review. Once initial mitigation plans are in place, the plans will need to be tracked and controlled as part of a regular Risk Management process. Risk mitigation plans will need to be revised in accordance with changing parameters and conditions affecting risks. Periodically, the entire risk mitigation plan portfolio needs to be reviewed for interdependencies and system changes.

  Mitigation strategy planning has many parallels with program and project issues planning. The key difference is that risk mitigation plans entail proactive, future-oriented selection and analysis of events with interactive effects. Mitigation analysis and planning examines root causes and seeks to perceive patterns and interdependencies with significant potential impact.

3.7.6 Team Risk Review

While the above steps toward government/contractor partnership can provide key results, there is a more structured process to assure the durability and completeness of Risk Management discussions between government and contractor.

Organizations where the stakes are high find that solid partnerships between government and contractor pay essential dividends. These include programs where delivery is highly visible, political, and innovative while the margin for error is low (for example, financial margins, low tolerance for re-planning, or critical customer needs prevent much variation in functionality).

In these cases, there are real benefits to a regular Team Risk Review—a forum where joint government/contractor risks may be identified, analyzed, prioritized, planned, and tracked. A regular Team Risk Review meeting brings together government and contractor program managers' current top risks; maintains continuity between these risks and those that were most important at the last meeting; assures common understanding of the status of the most important program risks; reviews existing actions; and assigns new actions as needed.

When regularly held with conscientious participation by both program managers and key staff, these meetings result in increased levels of candor and constructive momentum in government/contractor Team Risk Management. Eventually, experience shows that such a high-performing Team Risk Review ultimately fosters better program integration, improved reliability of program results, and increased sophistication in definition and development of analytic tools and measures.

The periodicity of the Team Risk Reviews will be determined by program needs, and will range from monthly to quarterly. In a complex program working under accelerated time-frames, and with multiple and unprecedented design features and functionalities, monthly meetings are recommended. In any case, meetings should occur at least quarterly to achieve successful results.

3.7.6.1 Team Risk Review Charter

As with any collaborative team that needs to have an integrated purpose, goals, and courses of action, the Team Risk Review benefits from having a Team Charter. This document may seem to reside in the "optional" category, but experience shows that charters actually build team clarity, cohesion, and efficiency through the explicit identification of specific agreements.

Useful topics to include in the Team Risk Review Charter are the team's statement of purpose, sponsor(s), membership, goals/outcomes targeted, stakeholders, strategic linkages, rules of engagement (especially decision rules), and measures of success.

3.7.6.2 Team Risk Review Agenda

Every Team Risk Review will naturally want to create its own agenda, but there is an SEI template that can be used as a starting point.[3] A recommended template includes:

1. Roundtable: Identify new or complex factors affecting the team and its ability to be successful in achieving success; e.g. changes in the critical path, emerging opportunities, linkages to other divisions or systemwide with impacts to or by the Team Risk Review, etc.
2. Report on TRR actions: Check to assure ongoing rigor in accomplishing critical risk activities.
3. Review status of all shared government/contractor risks.
4. New risks: Identify, discuss, prioritize, and assign actions. (This discussion may address risks that are germane primarily to government or contractor but it is useful knowledge for both, and may include shared risks).
5. Systemwide risks that require division attention: Examine multiple factors, root causes, and other relevant dynamics affecting systemwide/divisional risks, and assign any necessary actions.
6. Discuss specific segment priorities and planned risk activities, and assign any necessary actions.
7. Review assigned actions and select the next TRR date.
8. Evaluate the meeting (resulting in enhanced practices and efficiencies) and adjourn.

[3] See Appendix A.4, "CCD Team Risk Review, Sample Agenda."

3.7.6.3 Team Risk Review Guidelines

As part of the overall Risk Management process, Team Risk Management can provide an effective, multi-perspective forum for ongoing foresight and candid exploration of downstream risks. To be truly successful, though, Team Risk Management must itself be built on a solid foundation, including the success factors for Risk Management and the protocols for Team Risk Reviews.

The success factors for Risk Management are the following:

- well-developed and thorough installation of Risk Management in the government organization for management of government project risks (not just contractor risks)
- open, candid discussion and capability to surface risks, through a communications infrastructure agreed upon by government program managers
- understanding and commitment by both government and contractor that ultimate insight, accountability, and project outcomes are the responsibility of the government, though responsible government and contractor organizations will engender collaborative partnership in Risk Management to the full extent possible

The protocols for Team Risk Reviews are the following:

1. Startup TRRs need to meet monthly, either in separately designated TRRs or as a regular agenda period in other regular "working"—not just status—meetings. These initial meetings are in-person, face-to-face meetings, and occur for at least the first six to eight meetings, and preferably for at least the first year.
2. "Working" meetings are defined as sessions committed to open discussion, with surfacing of problematic topics when necessary, and allowing for voicing of multiple perspectives. These meetings develop sound decisions based on consideration and integration of important information—in a phrase, mature operation of "knowledge management."[4]
3. During these initial meetings, decisions will need to be made on such issues as: What communication needs to be open? Who needs to attend the TRRs regularly? Who will do the actual logistics and maintain the knowledge repository for the TRR—government, contractor, or both? Who decides what is a risk? What risks are priorities? How are decisions made? What are the necessary linkages between government and contractor Risk Management processes?
4. Once the TRR is well-established, an atmosphere of trust and candor has been established, and the risk environment for the TRR is well-distributed among, and understood by, all the TRR members, TRRs may consider using videoconference "dialogue/exchange" working sessions. These may become bimonthly, depending on the effectiveness of interim communication mechanisms.
5. Online communication as a vehicle for interim communication between TRRs is essential to successful Risk Management, and provides benefits from risk data input by all the designated TRR members. This online communication amplifies, but cannot substitute for, dialogue/exchange meetings.

[4] For a further discussion of knowledge management, see chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

6. Even where videoconferencing meetings have been established and operate effectively (equipment operates properly, participants are practiced in use of the form, appropriate logistics are in place, etc.), the TRR needs to meet at least quarterly in face-to-face meetings. The TRR can use these to address tabled issues, to think through any controversial and complex issues, to bring on board any new staff members to the TRR process, and any new business—especially risks that have controversial aspects or complexities—that would benefit from real-time collaboration.

7. For videoconference TRRs, the following logistics protocols will need attention:

   a. Meeting management roles (e.g., facilitator, scribe, timekeeper) need to be assigned. Videoconferences will need a facilitator *at each site.* At least one person should be present who is very familiar with operating the VTC—don't assume the equipment will work without knowledge.

   b. The following materials are needed *at each site:*

      - agenda
      - Risk Management tracking tools and charts. Documentation at each site is required—the quality of VTC graphics cannot yet be trusted for clarity.
      - minutes and actions from previous meetings
      - other materials, information, background data, etc.

   c. Points of contact/coordination should be identified, including who designates agenda topics for each meeting, and who takes the lead to make sure materials are sent out in advance.

   d. Special handling and logistics should be resolved. Duplication of materials for VTC can be a cumbersome task and must be performed in advance at each site.

   e. Equipment needs should be resolved. In addition to an overhead at each site, useful equipment in each conference room (or in a very accessible location) is a *telephone* and *fax machine* in the event of late-arriving documents that need to be examined by all participants.

8. A disciplined Risk Management process is especially needed at videoconference TRRs, and includes:

   a. surfacing of new risks

   b. discussion and decisions on acceptance of new potential risks

   c. prioritization and planning for new accepted risks—or assignments to perform these and return to the TRR for discussion/decision

   d. ensuring that government/contractor information/communication linkages are working well

   e. feedback on how well the Risk Management and the TRR processes are working, and decisions for remedy if necessary

   f. information on systemwide and interface information with impact on this organization's Risk Management

9. All Risk Management activities—including TRRs and interactions among project staff and between projects—need to be fused into a coordinated, comprehensive whole system that aligns with management of the programs and with system-level concerns.

10. Finally, disciplined Risk Management must never be interpreted to mean that discussion and dialogue are extraneous to the TRR. This level of open communication is the critical success factor for ongoing Team Risk Management.

3.8 Culture, Change Management, and Infrastructure

3.8.1 Corporate Culture and Its Impact on Successful Installation of New Initiatives

Organizational culture is a now widely recognized dynamic that affects operations, technical/business success, and the climate experienced by all staff from the time they arrive at work to the time they leave for home—and sometimes extends beyond the workplace. From the workbench to the executive suite, "culture" has become accepted as a force to reckon with, whatever the mission and goals of an organization may be.

Nevertheless, there are many different definitions of "organizational culture," all of which have some merit and utility. Especially relevant are those that involve working to install new initiatives, whether they are related to new technologies, improvement efforts, re-engineering or reorganizations, or new approaches to program management.[5]

Edgar Shein, foremost culture specialist and professor of management at MIT's Sloan School of Management, notes at least six meanings commonly held for organizational culture:

1. observed behavior habits (e.g., people are usually five minutes late to meetings)
2. norms that guide behavior (e.g., "the day stops at 5:00 p.m.")
3. core and/or dominant values that are both "espoused theory" by an organization ("we always deliver excellence") and "theory-in-use" ("when project schedules get tight, something has to give"). These distinctions are based on the work of Chris Argyris, a leading organizational expert.
4. guiding philosophy (e.g., "customer focus is our most important principle")
5. rules of the game to get along in the organization (e.g., promotions go to those who cause no waves rather than those with the most management skills)
6. feeling/climate of the organization revealed by such visible symbols as physical layout and interactions with those from outside the organization

All these, Shein maintains, are not actually culture but rather aspects of culture—and the most useful definition is actually the following:

> Culture is the deep level of "basic assumptions, values, and beliefs" taken for granted by organizational members, that have been jointly developed to (1) ensure survival in the external environment and (2) solve internal problems of

[5] See Appendix A.5, "Culture and Sponsorship: The Key Essentials for Managers to Create a Risk Management Culture."

integrated performance. Culture is like "water to fish," barely noticed by those living within it.

This definition implies that organizations often (perhaps usually) base their standard ways of performing on a reasonable *past* assessment of their basic needs for organizational success. To change culture, then, challenges a *modus operandi* that seems to organizational members like "the smart things to do" and is deeply entrenched in every aspect of organizational life. In other words, organizations make what seemed to be smart decisions at one time; to change these original decisions requires rather thoroughgoing and effective change management.

In addition to a definition that presumes organizational culture is all one thing, the reality is that every organization has multiple cultures—the culture of military and government-based employees, for instance, contains highly varied assumptions and values about how best to engender respect and lines of authority. Each division has its own culture—some value open discussion, others value presenting the boss with critical information and relying on that leadership for sound decisions. These multiple cultures may also be in contradiction with the overall organizational culture.

However, to bring the greatest clarity to this discussion, the core issue in dealing with culture is to step back periodically and take an objective, thoughtful look at what assumptions seem to be driving decisions and ways of doing business. The next step is to determine what aspects of the culture(s) are supporting the mission and goals at the present time, and what aspects may need to be brought into alignment with the future directions of a given organization.

The core question is this:

> *Do certain critical aspects of the corporate culture need to be changed if the organization is to continue to be successful?*

A useful guide to cultural examination is provided by Eric Flamholtz, professor of management at the Graduate School of Management, University of California, Los Angeles, who emphasizes the importance of assessing cultural impacts against corporate business goals. It's necessary to define specifically what must change, and what aspects, on the other hand, may actually support or which are neutral to successful outcomes, or which can be creatively aligned to support new directions.

For the NRO, assessments that address just these cultural dynamics have already been done. The NRO Jeremiah Report of Aug. 26, 1996, addressed nine key arenas critical to leveraging the NRO successfully into the 21st century: mission, systems, resources, management, oversight, acquisition, security, organization, requirements, and customers. In each category, there were profound changes made in the way the NRO has traditionally done business; moreover, the panel identified further changes that would be necessary in each area for a successful 21st

century NRO. These nine areas, taken as a composite, speak to significant levels of culture change. In particular, the Jeremiah panel pointed to the need for resurgent effectiveness in special NRO business practices and processes as critical to innovation; the development of proactive intelligence systems; and successful response to the "imperatives for near-continuous global coverage, long dwell, and hard-target characterization."

As additional culture data, the Baldrige study in 1996-97 targeted issues that continue to be validated by many inside the organization. This includes, notably, a need for a culture that supports integrated perspectives and an environment that reduces polarization. In particular, the Baldrige findings pointed to a need to move from "risk avoidance" to the kind of open communications that elicit widespread, knowledgeable information-sharing.

Indeed, a culture that once may have served the organization very well now appears to stand in the way of NRO effectiveness and a forward readiness that is alert and proactive to risks and managing them effectively. Many indicators in the assessments that examined NRO culture are in the direction of the Risk Management efforts that have been engaged at IMINT.

Risk Management experience has shown that, for most organizations, Risk Management requires some culture change. A key factor in why Risk Management is not naturally and widely practiced in supporting organizational success is that Risk Management itself challenges widespread U.S. cultural assumptions. Risk Management requires identification of "bad news that hasn't happened yet" in an overall culture that seeks the positive and focuses on the present, not the future. No wonder then that changes in some critical aspects of culture are needed to achieve the level of open and forthright communication that may be initially very disconcerting to organizational leaders and members.

Therefore, in working to change or manage culture, leaders and others in organizations are well-advised to practice patience, planning, and validation of progress when it occurs—all of which require effective culture change management.

3.8.2 Change Management

3.8.2.1 Culture Change and Resistance

As with definitions of culture, there are widely varying perspectives on what to do about organizational culture and its impact. Since the period when quality leader Deming's "16 Principles" have become broadly recognized (and sometimes adopted) by U.S. business, organizational culture has been addressed as both support and hindrance. A little-remembered caution of Deming's was that changing organizational culture takes time: usually five years. Yet when working to improve our organizations, frequently that reality of organizational evolution is lost —often in well-meaning but over-hasty or over-engineered approaches to change.

The result of efforts that fail to take into account respect for the existing culture in launching new technologies or new approaches—as well as careful planning to work as much as possible in accord with the culture—is resistance. Indeed, resistance can be viewed as a natural response to new things. Yet Dr. Erik Winslow, chair of the Department of Management Science at George Washington University, maintains, "People do not resist change. We actually change all the time. Many changes we welcome. What people resist," he says, "is their fantasies of a negative future." In fact, social science research increasingly reveals evidence that change enacted as a 'good fit' with the culture is likely to succeed. "People support what they help create," and "leaders who want to manage successful change of any kind need to be ready to clarify their vision for the ideal future, and to repeat that vision over and over."

3.8.2.2 Effective Change Management

Whatever the cultural dynamics, the "negative fantasies" people have about new things usually include the fear of key losses—loss of control, opportunities, ability to use proven skills, potential growth, flexibility, self-esteem, credibility—as well as concerns about applicability (the "not invented here" syndrome) and ultimately, the fear of organizational failure.

Successful change management results from leveraging a portfolio of guidance in knowledge and actions that must operate in concert. The SEI approach to Risk Management rollout and installation includes respect for this guidance. As Machiavelli said, when asked what was the best approach to inculcate change, love or fear: "Love lasts longer; fear is quicker." A natural tendency on the part of leaders is to "get it over with," reasoning that a long drawn-out process of change is more destructive than quick action. However, there is a middle ground—as many organizations are finding.

This middle ground involves treating new practices, technologies, and initiatives with a reasonable level of planning, and—the essential ingredient—communications. As General Bill Creech, the four-star general who reformed the Air Force Tactical Air Command, said in his "15 operational principles for change":

1. Have an overall theme and purpose.
2. Use goals throughout—and talk about them regularly.
3. Measure productivity.
4. Have leaders at many levels.
5. Instill responsibility.
6. Reward success.
7. Build a climate of pride.
8. Build a climate of professionalism.
9. Inspire organizational discipline and loyalty.
10. Provide everyone with a stake in the outcome.
11. Educate, educate, educate.

12. Communicate, communicate, communicate.
13. Make it better.
14. Make it happen.
15. Make it last.

3.8.2.3 The Importance of Strong Sponsorship

Above all, there must be both an engaged management and a culture that genuinely encourages the foresight and open communication that Risk Management requires. The cultural change challenges the traditional assumptions and management paradigms of many organizations, yet open information on specific divisional risks is essential.[6]

Gen. Creech's principles also imply a critical ingredient in effective change management that he himself exemplified in his "15 principles"—that is, solid sponsorship. He voiced his goals and reasons for them often. He was the prime driver behind those principles—rewarding, holding people accountable, being a model for what he expected others to do.

In Chapter 5, "Rollout, Installation, and Infrastructure," there are several examples where strong sponsorship at IMINTmade the telling difference between adoption and what some refer to as "malicious compliance" (participating just actively enough or just long enough to allow a new initiative to complete its cycle and move on). One example is the decision by the EIS director to make clear his sponsorship for Risk Management by conducting an Executive Risk Clinic and establishing the EIS System-Level Risk Management Team (ESRT).

There is a significant role that leaders can play in accelerating change initiatives—not the "hammer" approach but one of authoritative communications. Clear and consistent direction and support throughout all meetings and interactions avoid the danger of mixed or missed messages. A guide to defining precise actions that leaders can take to propel their organizations forward to a strong Risk Management culture is provided in the Appendix.[7] A brief summary of these key actions is below:

- What gets tracked and measured gets performed.
- Open communication means "not killing the messenger."
- Successful sponsors model desired behaviors.
- Public rewards, but even more importantly, adequate resources to support are vital.
- Performance criteria are specific and targeted to desired results.

---

[6] For an excellent discussion of this subject, see Appendix A.2, "Encouraging Winning Risk Management Behavior: The Exercise Left to the Student," by Art Gemmer and Philip Koch from the 1997 Risk Management Conference.

[7] See Appendix A.5, "Culture and Sponsorship: The Key Essentials for Managers to Create a Risk Management Culture."

3.8.3 Infrastructure

To leverage "making it happen" and "making it last," building an infrastructure to support any change effort is a highly effective approach. Especially for new initiatives that are creating a change in the culture, building a solid, well-designed infrastructure to support the change may initially seem burdensome. However, the infrastructure itself—if well planned—often becomes a value-added support for new efficiencies and benefits to other program activities. Once established, the Risk Management infrastructure becomes seamlessly integrated into program operations.

The Risk Management rollout and installation process applied at IMINT, as seen in the later actual experience descriptions, provides a tailored infrastructure designed by the organization to help create Risk Management awareness and practice.

Initial steps in the rollout and installation to build the Risk Management infrastructure include

- establishing the risk baseline to identify risks
- conducting Risk Management education in order to (1) provide a comprehensive overview of the Risk Management process, (2) ensure that all members of a given division or team are "on the same page" with common language and expectations for Risk Management, and (3) provide clear guidance on what a "Risk Management culture" requires in acquisition organizations
- defining, through a Risk Clinic or parallel activity, the tailored Risk Management process for each specific division, which may result in: government Risk Reviews; government/contractor Team Risk Reviews; regular agenda items in existing forums; or even informal processes of capturing and presenting risks for discussion and planning at regular intervals
- establishing effective system interfaces and a system-level forum (see discussion below of the executive-level Risk Management infrastructure) to ensure disciplined management of system-level risks and their mitigation plans
- establishing a systematic methodology to ensure that senior management is kept well informed, and in turn provides the leadership, sponsorship, and guidance necessary for the Risk Management infrastructure and processes to operate smoothly and effectively

A note of caution: a curious but inevitable result of successful Risk Management can and usually does occur, when one or more divisions becomes proficient in Risk Management, while others are still considering how deeply they would like to engage in that culture shift. The advanced Risk Management practitioners become more candid in other forums as well; they become better able to present logical, credible cases for requests for resources, programmatic changes, etc., based on their thorough risk analysis and mitigation planning. This can be seen as a threat to divisions/units that have not fully engaged in Risk Management. However, for an organization serious about Risk Management, this kind of culture leadership should be seen as an asset and model for future development across the organization.

3.8.3.1 Executive-Level Risk Management Infrastructure

The executive forum on Risk Management eventually depends on the robustness of each division-level Risk Management effort to create a sturdy process at the executive level. What this means in practice is that—while there is synergism between divisions and their executive forum—there is also a gap in the executive forum should any division(s) lag behind in their Risk Management process.

Furthermore, strong sponsorship for the executive forum is the most critical. Stable, committed, actively involved senior leadership is essential for an executive Risk Management forum to be successful. A worthwhile criteria for the executive forum is that it be established in such a way that a senior leader can be present for every meeting, preferably with continuity across a series of meetings.

In addition, an executive Risk Management forum has aspects that distinguish it from other executive sessions—the open dialogue required for successful Risk Management does not lend itself to a "status report" type of meeting. Executives engaged in Risk Management need to discuss not only risks but opportunities; examine performance, cost, schedule, and other relevant factors in real-world terms; consider executive-level tradeoffs with impact on ultimate program success as well as political impact; engage in alternative scenario planning and cost-benefit analyses derived from these tradeoffs; and come to decisions on mitigation strategies that include contingencies that may require more innovation than the risk mitigation strategies that they are designed to follow. Because Risk Management, finally, involves examining the uncertain future, strategic thinking needs to be applied to pragmatic possibilities.

Therefore, the infrastructure for the executive Risk Management forum—wherever it is installed—needs to include open discussion of the full range of potential and already identified risks, including business, management, technical, and political factors. The executive forum also requires a high tolerance for behaviors and dialogue unfamiliar to many executives and uncomfortable to most—that is, the willingness to engage in discussions where the "one right answer" is not available. The usual management "can-do" attitude (and even more importantly, the expectation of a "can-do" attitude) by program and technical staff must be relaxed. Executives must refrain from "killing the messengers" or necessarily requiring a solution when a risk is raised. A value needs to be placed on the uncomfortable issue being raised.

As a result of these cultural developments, in addition to the overall cultural need for support of Risk Management, many leaders find that they have an additional specific set of challenges to behave in ways they have been taught to avoid, and to overturn familiar and comfortable patterns of operating.

4 IMINT Goals for Risk Management

The mission of the NRO, "to enable U.S. global information superiority, during peace through war," means that NRO has responsibility for leading technology innovations. These are often unique, breakthrough technologies, with significant impact on the future of U.S. intelligence and military support.

"When the American government eventually reveals the (full range of) reconnaissance systems developed by this nation, the public will learn of space achievements every bit as impressive as the Apollo moon landings. One program proceeded in utmost secrecy, the other on national television. One steadied the resolve of the American public; the other steadied the resolve of American presidents." (Albert Wheedon, quoted by NRO Director Keith Hall in a speech before the Naval Research Laboratory, June 17, 1998.)

As a major organization supporting the NRO mission, IMINT is charged with contributing to activities that include "unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems and related intelligence activities." (NRO Web site <URL: http://www.nro.odci.gov/background.html>.)

In response to these critical challenges, IMINT launched its original government-focused Risk Management effort. IMINT leadership identified several goals that were instrumental in the decision to pursue this course of action. As outlined in the preface to this document, NRO Deputy Director Dave Kier determined specific areas for improvements in acquisition, risk, and program management. Accordingly, Kier decided to begin the improvement strategy with the IMINT Risk Management initiative. Based on the strategic partnership with the SEI, this initiative was designed to achieve gains in several important ways, including the following:

- provide a fundamental, positive impact on the way NRO pursues its software-intensive business
- provide a highly leveraged return on investment by capitalizing on the efforts of others
- provide ready access to leading-edge solutions that are applied and pragmatic

EIS Program Director Al Krum refined these goals further to address specific needs identified at IDP. These goals were intended to

- establish a consistent, durable, and effective Risk Management process to support program success

- provide proactive visibility into program risks to mission partners and other external stakeholders
- communicate to contractors how the government identifies, prioritizes, and deals with program risks, so that they can be clearly engaged in overall mission success
- utilize Risk Management to communicate across system program concerns, coordinate between segments, and analyze and work together on interdependencies
- accomplish all of the above, change the culture from one in which leaders and contributors assume that concern about risks can be postponed to "when we get there" to one in which everyone anticipates and plans toward areas of risk

4.1 Statement of Need for Risk Management at IMINT

The decision by IMINT leadership to pursue Risk Management was in direct response to the factors, challenges, and current environment that IMINT must manage to produce successful systems. As Command and Control Division Director August C. Neitzel outlined in his presentation to the 1998 SEI Symposium, IMINT leaders based their decision on the following:

- IMINT systems are increasingly complex and interactive, requiring disciplined, comprehensive Risk Management for successful progress.
- Successful program delivery requires identification and understanding of the interrelationship of risks within and across programs; risks in one element can give rise to risks (or actual realized problems) in another element.
- Risks not proactively managed will eventually create their own negative consequences.
- Early risk identification, analysis, and mitigation can reduce downstream surprises and problems.
- Shrinking budgets and tighter schedules virtually eliminate any margin that could previously be retained and available to offset problems that inevitably occur late in a program.
- IMINT had experienced several severe programmatic surprises, spurring a commitment to reduce unexpected events and delays.
- System Risk Management held the promise of creating a viable "trade space" among IMINT divisions with regard to funding and scheduling.
- Risk Management discipline and communication enables articulation of risks to executive management.
- EIS/IDP Risk Management provides an example of best practice for IMINT.
- EIS/IDP Risk Management provides an example of best practice for the NRO.

EIS Program Director Al Krum, in direct response to the urgent need to establish effective Risk Management at IMINT, decided to mobilize rollout and installation efforts rapidly. Accordingly, he directed that system-wide activities be scheduled for completion by September 1998. This accelerated timeframe was designed to communicate the serious commitment of

the EIS program director to support program success through application of Risk Management.

5 Rollout, Installation, and Infrastructure

Rollout and installation of a full Risk Management system process was begun. It built on the foundation outlined in Chapter 3—that core processes arrive at core results for Risk Management—and based on the goals for Risk Management as determined by IMINT leadership. This chapter reveals how the core processes of Risk Management were installed at IMINT.

With certain system-wide, consistent practices in place, Risk Management can be practiced in a variety of ways, and can be tailored to individual divisional and organizational needs. In answer to the question, "How should I do continuous Risk Management?" the authors of the *Continuous Risk Management Guidebook* have said:

> *"Risk Management is simply an area of emphasis of everyday business. It should be ongoing and comfortable. Like any good habit, it should seamlessly fit into your daily work. ... There is no one special set of methods, tools, or communication mechanisms that will work for every project. The key is to adhere to the principles, perform the functions, and adapt the practice to suit your needs"* [Dorofee 96].

The IMINT rollout, installation, and infrastructure were, in fact, specifically tailored for the IMINT environment, its divisions, and the system delivery program there. The overall process was designed to achieve the right mix of consistent, standardized processes at the system level, together with "local options" within the divisions. This was accomplished in a context in which program delivery schedules were tightly constrained and budgets were disciplined.

To achieve rollout and installation in a dynamic, vibrant system such as IDP required that IDP leaders and contributors step up to the challenges inherent in new processes. Across the program, there were many contributors who committed their best efforts to achieve successes in Risk Management. Their stories are worth reading for indications of the compelling variations that dedicated participants can use to shape Risk Management effectively, and achieve significant results.

Everyone involved in the SA-CMM assessment at IMINT agreed that there were useful findings provided, including recommendations from the joint NRO/SEI team for full-system acquisition improvement. At the same time, IMINT leadership recognized the urgent need for near-term support for IMINT programs. As a result, IMINT leadership decided to focus first on an SA-CMM Level 3 Key Process Area, Acquisition Risk Management. Once the decision

was made, the next step was to develop a plan for rollout and installation across the organization.

The EIS director was convinced that a thorough, streamlined approach, as accelerated as possible, would provide best value and disrupt operations the least. He therefore mandated that all EIS divisions conduct a Risk Management training session from the SEI Continuous Risk Management course, tailored specifically for IDP, and titled "IDP Risk Management Training." Pursuant to their Risk Management Training, divisions could decide whether to undertake a Risk Clinic to define their Risk Management process. As described below, three of the five divisions decided on this approach.

To convey his strong commitment to Risk Management, the EIS director further decided to provide leadership in the process by holding an executive-level Risk Clinic in which all division directors would participate. Following the Risk Clinic, the EIS director created an EIS System-Level Risk Management Team (ESRT), made up of all division directors and attended by key technical people as well, which was to meet monthly. Therefore, the executive leadership pioneered the system-level rollout and installation.

The pilot Risk Management program at IMINT was launched in June 1997, following the SREs that were held in January and April 1997. The actual rollout and installation of Risk Management throughout the rest of the organization began in January 1998 with the Executive Risk Clinic, and was completed in September 1998, with the last EIS Risk Management training session—nine months of initial installation activity, supported subsequently by expert guidance and maturation of the Risk Management process in each division and the ESRT.

The following section describes specific information on the EIS Risk Management rollout and installation.

5.1 Pilot Program at IMINT

The pilot program, as is true with any pilot, experienced significant visibility. The CCD director and his area managers were highly oriented to program success. Their criteria for deciding to move forward with the Risk Management pilot was simply: "will this provide value to our likelihood of achieving the highest-quality program results?"

Actual progress toward rollout and installation in the pilot organization entailed candor, negotiation, and open communication from the very start. A number of documents have already been written outlining the experiences of, as well as the procedural approaches to the CCD pilot program, including "Managing Risk Management" by August C. Neitzel [Neitzel 98].

For this section about the pilot program—in keeping with the emphasis on multiple perspectives for sound Risk Management—comments and insights were solicited not only from the

CCD director but from area managers and contractors as well. This section draws on that compilation of inputs.

5.1.1 Pilot Program Selection Rationale

IMINT leadership selected the Command and Control Division (CCD), a division within IDP, as the initial pilot program. There were at least three reasons for this selection. First, the division was the most software-intensive program within IMINT. IMINT leaders saw a close relationship between the division's efforts and the traditional focus of the SEI and its Risk Management expertise. Second, this division had experienced several setbacks and was seen as most able to profit from immediate installation of Risk Management. The division generally, and the division chief in particular, were seen as the most skeptical in IMINT. The belief was that if Risk Management could be successful here, rollout across other IMINT divisions would progress relatively smoothly. Fourth, since the initial assessment at IMINT was viewed from a software perspective, there was a belief that this division would most appropriately serve as a startup for Risk Management at IMINT.

5.1.2 Initial SREs and Risk Identification Process

To launch the Risk Management pilot, two parallel Software Risk Evaluations (SREs) were conducted, one with the participating contractor Lockheed Martin in January 1997, and one with the government division itself in April 1997. The scope of each SRE was bounded to the same jointly performed program, given the following criteria:

- minimize potential disruption to more time-critical activities
- focus on an activity early in its acquisition process so that it might more easily incorporate new Risk Management practices
- apply Risk Management to an activity where cultural differences were most evident

Findings from the contractor SRE were privileged and confidential and so are not described here, though key findings have been included in the joint government/contractor Team Risk Review planning and tracking of risks.

The government SRE revealed 10 risk areas for the division:

1. requirements
2. staffing
3. integration and test
4. design
5. schedule
6. transition to operations and maintenance
7. program office management

8. commercial off-the-shelf (COTS) software
9. prime/subcontractor relationship
10. contract management

Of these, risk areas 3, 4, 6, and 8 were selected for the division to address. The other areas, while judged important, were considered to be outside the sphere of influence of the division, and consequently would be difficult to address and would provide the division with a low return on investment for risk mitigation. (It is worth noting that later in the division's Risk Management process, some risks in these areas arose and were raised to system-level attention. This helped foster support for the rationale to create a system-level Risk Management effort.)

The SRE performed on the government division narrowed the area of concentration, and revealed to the pilot program its portfolio of identified risks. In fact, the 10 original risk areas contained an initial list of 77. This number was further reduced to a priority list of 30 interrelated risks that the division planned to track and control on a continuous basis.

The results of the two SREs were brought together at the first Segment 4 Team Risk Review in the form of the top government and contractor risks defined in each SRE. Recognizing the importance of the improved partnership between the government and the contractor, then-EIS Director Fred Doyle had as a principal goal to launch the Segment 4 joint government/contractor Team Risk Review (described below).

5.1.3 Initial Team Risk Review

Beginning in June 1997, the division immediately initiated a monthly series of joint government/contractor Risk Management meetings, called Team Risk Reviews (TRRs), prior to installing a self-standing government Risk Management process.

The pilot division initially chose not to follow the SEI recommendation to hold a Risk Clinic (described the following section). There was an early conviction that the division could quickly adopt a Risk Management process that would be rational, operational, and effective. The division chief and his section chief, who was most involved with Risk Management, later openly discussed as a "lesson learned" that they benefited greatly when they eventually held a Risk Clinic, and they questioned their initial reluctance to engage in the clinic activity. (See Section 6, "Lessons Learned.") The division chief and section chief said they thought they understood which Risk Management approach would be most successful for them and their contractor. However, they said they quickly discovered a number of obstacles to effective joint government/contractor Risk Management, including

- various domain and cultural backgrounds
- differing Risk Management knowledge bases

- a lack of clear, joint government/contractor purposes and goals for their program's Risk Management effort
- a tendency for group members to operate from their own, differing assumptions and expectations about how to execute Risk Management

The communications difficulties and unresolved focus resulted in meetings that were deemed difficult for all concerned—government, contractor, and SEI facilitators. This led to a critical negotiation wherein both government and SEI participants identified gaps that both saw as detrimental to critical success factors. Together, the division leaders and SEI participants developed a "restart" approach that included conducting a Risk Clinic to define precisely the divisional end-to-end Risk Management process.

5.1.4 Risk Clinic

The diagram on the following page portrays the CCD Risk Management process at a high level, as it has been consistently followed (with some modifications to align it more closely with useful practice) since the CCD Risk Clinic.

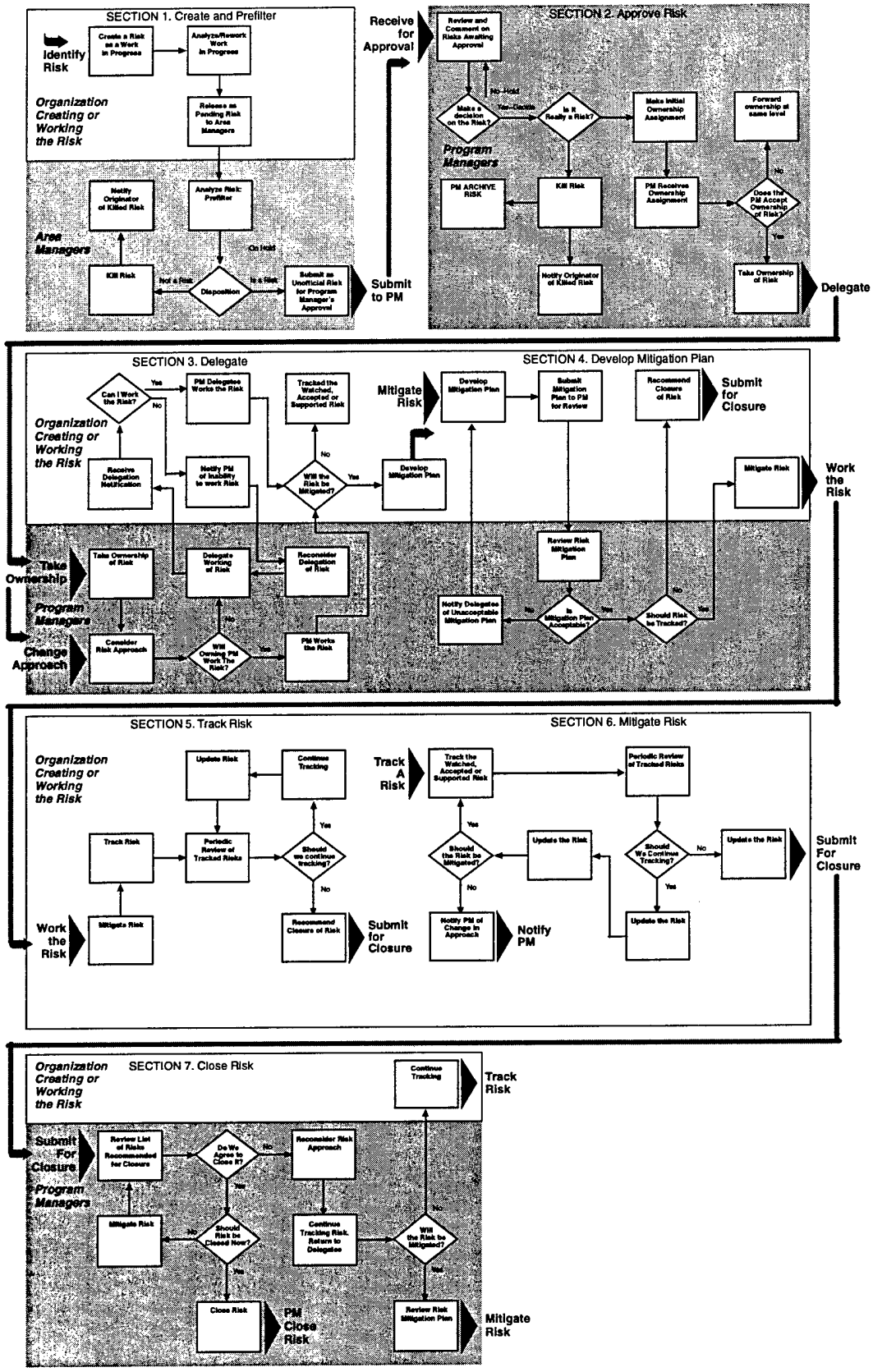


Figure 6: CCD Risk Management Process

Figure 6 (continued): CCD Risk Management Process, Legend for Preceding Chart

SECTION 1. Create and Prefilter

Any program office/team member granted tool access can identify a risk and initiate the risk management paradigm. As much known information regarding the risk condition, and it's consequences in a concise "Risk Statement" is input as well as initial assessment of probability, impact magnitude, and likely timeframe of action needed prior to the Risk becoming a problem. The Area Managers will perform an initial analysis ensuring additional programmatic and system engineering information is considered prior to submittal as a unofficial risk to the PM.

SECTION 2. Approve Risk

The Program Manager will ensure all program information is appropriately considered and assign and delegate ownership of the risk for appropriate potential action: Kill, Mitigate, Watch, Accept or Transfer.

SECTION 3. Delegate

Area program managers and program office personnel will initiate action with respect to the risk and its attributes, of probability, impact, and timeframe. This is and iterative process that results in discrete activities regarding the risk according the division's risk management plan. Note: Supported in the context of
the tool, must first be "supported" i.e. the desire and resources assigned to allow mitigation.

SECTION 4. Mitigate Risk

Developing the Mitigation Plan is a typical Plan, Do, Check, Act set of activities that are managed as any typical program office initiative. The key distinction is that these activities were initiated by as a negative consequence identified as potentially occurring in the future and the activities are oriented at reducing or eliminating this potential negative consequence.

SECTION 5. Track Risk

The Risk and its associated assigned decision attribute (Kill, Mitigate, Watch, Accept or Transfer) is monitored. Periodic status is provided at normal program office meetings. Updated status information is provided by the risk owner and monitored by the Area Managers and the Program Manager.

SECTION 6. Example: Track Risk

This is an example flow of how a risk and its assigned decision attribute: Mitigate, Watch, Accept or Transfer would be tracked.

SECTION 7. Close Risk

The process for the closing a risk is iterative and allows for reconsideration regarding mitigation, continued tracking or final closure.

The division decided to hold its Risk Clinic in September 1997. In this day-and-a-half process, the division, with SEI assistance, "red-lined" the SEI Risk Management process architecture to suit its specific divisional needs and ways of doing business. Conducting the Risk Clinic served a number of purposes:

- It provided a forum for team design of the division's own documented, consistent process for divisional Risk Management, based on but not constrained by the SEI templates, which the team red-lined.
- It ensured that all team members understood not only the overall process but their own and others' individual roles in identifying, analyzing, prioritizing, and mitigating risks.
- It provided all team members with a common language and terminology, as well as criteria, defined by consensus agreement of all team members, which they could use to communicate effectively about their Risk Management efforts.

5.1.5 Establishment of Risk Management as a "Way of Doing Business"

With its Risk Management process defined, the team returned with a very different perspective on its Team Risk Reviews, and afterward met consistently on a monthly basis. This provided clear benefits in a number areas, particularly three key areas:

- The government and contractor personnel formed a team. Their communications about joint as well as separate risks reached a high performance level, wherein honest, open, and early disclosure about risks was valued, and problem-solving occurred free of blame and with commitment to finding the best solutions. Discussions on risks could merge the broad pool of talents, expertise, and experience from both government and industry.
- Based on their disciplined Risk Management analysis and planning, division members were able to formulate precise, logical, and compelling presentations for senior management to request appropriate responses and/or resources to meet mitigation needs.
- Rather than finding no avenue for communicating cross-divisional or system-level risks, the division can now contribute its technical perspective on system delivery to raise appropriately risks that must be considered at the system level.

In addition, to ensure that Risk Management was not just considered at one meeting a month but was instead integrated into daily business, one section chief initiated a weekly session, called the "Starbucks meeting." At these informal meetings, where participants usually stood and talked with coffee in hand, new risks were identified and division members effectively tracked and controlled existing risks.

This section chief has said, "The revelation here is that Risk Management is not only within the scope of our industry partners, but a clear part of the management tasks of the government team. The 'value-added' step changed the focus of the model to IMINT management outcomes. As a result of the Risk Management process, for the first time an IDP division chief could speak in objective terms about the risks to his segment within the context of risks to the overall EIS program. The change was one of moving from a reactive management process at the IMINT level to the highly desirable proactive management process that would vastly improve our chances of government management within the target costs and schedule for the EIS program—truly an advancement for the NRO."

5.1.6 CCD Risk Management Training

CCD had served as the pilot program, and had conducted successful Risk Management operations for a year, having had some members engaged in the initial Software Risk Evaluation, most of the team involved in the CCD Risk Clinic, and regular active team participation in the monthly Team Risk Reviews. In addition, CCD scheduled its own Risk Management training session in September 1998. This session was actually conducted after training sessions were held in other divisions where members had less practical Risk Management experience, but who were following the sequence defined by the EIS program director (see Section 5.3). CCD's decision was made for a number of reasons:

- It helped to bring on board new division members who had not been present for the SRE. Some new team members were unacquainted with the divisional Risk Management process or its underlying practices.
- It provided for a common language across Segment 4 and Segment 3. Segment 3 was a support division that had not been exposed to either the SRE or the division's Risk Clinic. It was struggling to align with Segment 4 and operate at high performance on Risk Management to provide seamless delivery.
- It helped to build a common language and dialogue with CCD's contractors. These contractors had been champions of Risk Management from the beginning of the pilot project, as shown by the active involvement of the contractor manager as a partner to the CCD chief. Although the contractor was already approaching a high level of team partnership, the contractor manager wished to more closely relate their two systems of Risk Management. Indeed, upon completion of the IDP Risk Management training session, the contractor redesigned its report templates, forms, and data-collection procedures to align with those of Segment 4.
- As a result of applying Risk Management practices such as regular risk identification and analysis (the "Starbucks meetings") and the Team Risk Review, the division chief decided to improve communications among all his staff by holding the IDP Risk Management Course. Not only Segment 3 but new members of the Segment 4 staff as well, who were attending the Team Risk Review, sought to "get on board" more rapidly with full communication and participation in Risk Management.

5.1.7 Initial Creation of the Risk Management Tool by CCD

As the division became more convinced of the value of Risk Management to improve the likelihood of program successes, division members continued to refine, enhance, and mature their process. One principal result was the development of an automated tool to enable further communication between Team Risk Review meetings, and to capture current activities as well as the overall database of risks being managed by the division.

This tool, initiated by the division chief and the manager he appointed to focus on Risk Management, was co-created through collaboration among NRO managers and two of their contractors, Lockheed Martin and Oracle, and was supported with input by SEI staff members. Development of the Risk Management tool (the "RMT") to facilitate government and contractor team communications was initiated by the division chief and his section chief in charge of Risk Management. According to this section chief, "Open communication is the hub of Risk Management. The value of the RMT is to expand (not replace) team communication, and in turn to support the Risk Management process."

The tool uses links to email to alert team members to queries and other requested actions, while helping to ensure that members handle appropriate tasks (e.g., managers have certain approval prerogatives, or mitigation action teams can be formed and members can communicate privately with one another about technical explorations until the information is ready for publication).

Development of the tool began in January 1998 and continued over the spring. It was gradually entered into use in the division as its functionality became available. By August 1998, the tool had emerged from its "engineering version" and had been improved with attractive graphics and increased ease of transportation and utility.

By July 1999 the tool had been demonstrated throughout EIS/IDP, and was presented at an early 1999 meeting of the senior-level Acquisition Steering Group. Following this demonstration, the EIS program director declared that the Risk Management tool would be the system-wide standard for each division to manage and prepare briefings about system-level risks.

The initial diagram was designed into a brochure used by CCD to inform others about the Risk Management tool and its functionality for Segment 4. While later tailored to align with the system-level Risk Management process, the original version was designed in accordance with the Segment 4 Risk Management process.

5.2 EIS System Risk Management

In fall 1997, after it became clear that the Segment 4 pilot Risk Management effort was established, EIS Program Director Al Krum announced his decision that system-wide Risk Management would be incorporated into standard business practices at IDP. To support this effort and symbolize his sponsorship, the EIS program director decided to have the executive level at EIS become "role models" for the organization by conducting an Executive Risk Clinic. This session was held in January 1998, and in March 1998 the EIS System-Level Risk Management Team (the ESRT) was launched. Thereafter, the ESRT met monthly, chaired initially by the EIS program director, and later by his deputy, Col. Stephen Wojcicki.

The ESRT in many ways exemplified both the goals sought by the executive level at EIS for Risk Management, and the challenges of executive Risk Management. Goals set for the ESRT were ambitious (see the "Original Goals" section below) and, as discussed above, were derived from experience and the knowledge that, without some forethought, system complexities would likely result in program deficiencies and possibly system failures.

However, since the ESRT was established prior to the rollout and installation across the organization of divisional Risk Management, there were widely differing ideas about what Risk Management should entail, and what results it should achieve. This continued until the entire EIS system level had aligned its practices and processes. This resulted in several months of a certain amount of confusion, and some difficulty with the system-level Risk Management process until each division had received Risk Management training and had installed their tailored versions of Risk Management.

In addition, the "open-dialog" forum essential to successful Risk Management was relatively unfamiliar to division chiefs as a group of leaders. Most system-level meetings involved status reports to senior management. Because of time constraints as much as unwillingness,

there was little opportunity for chiefs to engage in dialog among themselves. Also, although dialog did occur at divisional staff meetings, and although there was some contractor support for risk identification and planning, the lack of a "Risk Management culture" meant that widespread forecasting of risks was new to the program.

Over time, division chiefs expanded their arena for open discussion, problem solving, and making joint decisions on system-level risks and related issues. By late spring 1999, division chiefs began to discuss program impacts and possible trade-offs among program priorities, which is the core of effective system-level Risk Management.

5.2.1 Key System-Level Risk Management Startup Activities: EIS Risk Clinic, Establishment of the IDP Risk Management Plan, and the ESRT

Understanding that starting the process of system-level Risk Management would be no small feat, the EIS program director met with SEI project team members prior to the Risk Clinic to identify key factors and plan for the event. Among the considerations addressed during design of the Risk Clinic were the following:

- What are the strategic business priorities for EIS?
- How can Risk Management best support these priorities? (For example, one priority was to practice discipline among divisions to forecast schedule slips, especially those with serious potential impact on overall program delivery.)
- How will these priorities in turn affect Risk Management? (For example, an executive decision to fund a management reserve dedicated to offset known issues could be perceived as depletion of Risk Management reserves, unless goals for both were clear.)
- What kinds of messages does senior management want to send with regard to Risk Management, and how can these be communicated effectively? (For example, to what degree are divisions expected to participate in the system-level Risk Management process, and what will it take to make sure this happens?)
- As perceived by the leadership, what internal obstacles and supports exist relative to system-level Risk Management rollout and installation?

5.2.1.1 The EIS Risk Clinic

The EIS Risk Clinic was held on Jan. 6, 1998, and was attended by the EIS program director, all division chiefs, some technical managers, and a key contractor from the Development Systems Division. The EIS Risk Clinic provided an executive briefing on system-level Risk Management, keyed to the following SEI-standard "eight questions for managers on Risk Management":

1. By what criteria do you assess your program's success?
2. What are the top five barriers that could prevent your project from being successful?
3. How do you decide which of these is most important?

4. What decisions need to be made to mitigate these risks?
5. When do these decisions need to be made?
6. Who needs to be involved in these decisions?
7. How will you know if your actions are effective?
8. Do you believe these issues are being openly shared and understood?

The EIS Risk Clinic achieved the following outcomes:

- development of the IDP Risk Management plan, first iteration
- development of the IDP Risk Management transition scenario, to begin installation of Risk Management as an integrated process throughout the system
- an action plan with assignments to support leveraging the transition scenario

5.2.1.2 Establishment of the IDP Risk Management Plan

The initial IDP Risk Management plan (the complete and most up-to-date version is included in the appendix) contained a process designation of the already-established monthly Development Program Review (DPR) meeting as the site for regular system-level Risk Management. However, the DPR meetings routinely lasted four to six hours, were attended by an unwieldy number of people (50 was not an unusual number), and did not include, nor were they likely to include, time and space for an open forum for Risk Management identification, analysis, planning, or control.

5.2.1.3 Establishment of the ESRT

Consequently, the EIS program director decided to establish a monthly EIS System-Level Risk Management Team, the ESRT, to address directly system-level risks. These meetings were officially launched in March 1998 and continued monthly thereafter. Members of the ESRT were identified in the ESRT team charter. Attendance at ESRT meetings was usually no more than 10 to 15 people, including division chiefs, and the meetings were therefore able to accommodate substantive discussions.

5.2.1.4 Initial Goals for the ESRT

To develop awareness of how each division chief's goals could merge to form a cohesive set of goals for the ESRT, the following list was developed during early sessions in 1998:

- Create a common vision of Risk Management and success for EIS.
- Encourage a sense of win and value from Risk Management—indicators that Risk Management is actually preventing or mitigating system-level risks.
- Define what risks are indeed system-level, address those, and properly delegate those that should be owned and managed in divisions or at the IMINT level.

- Establish an enhanced capability and process in actual Risk Management that is distinct from but contributes to overall program management.
- Establish common information formats and cross-interpretive data descriptors so that division chiefs can assess risk information and make sound management decisions on risks.
- Establish and track system-level mitigation plans.
- Provide the EIS program director with the information he needs not only at the ESRT but at related program forums as well (including the monthly Development Program Review meetings).
- Establish a culture that supports proactive Risk Management.

5.2.2 System-Level Mitigation Strategy Planning

During the period when initial divisional Risk Management training sessions and Risk Clinics were being completed, the ESRT underwent a two-part seminar (in September and November 1998) on system-level Mitigation Strategy Planning (MSP). The MSP was conducted to provide a template for system-level risk mitigation that could be, as appropriate

1. delegated to project managers, technical leads, system integrators, or cross-organizational Integrated Project Teams (IPTs)
2. examined initially by the ESRT for system-level aspects, interdependencies, alternative potential scenarios, or cost/program trade-offs that require executive attention
3. or a combination of these approaches that was best suited to a particular risk or set of risks.

During the two MSP sessions, all current system-level risks were evaluated as to "payback/return-on-investment"—the value of an effective mitigation strategy for each risk, and the cost of mitigating each risk versus the cost if the risk becomes a *bona fide* issue. These two indices were built into a matrix to surface those risks that had the greatest potential yield as a result of mitigation planning, that is those with "high payback/low or medium investment."

One of these was selected for further analysis and mitigation planning by the ESRT members present. At the outset of analysis, many members indicated that they "knew there was only one way" to address that risk." As the session proceeded to elicit from each ESRT member the "one way," it became clear that each person's was different—yielding a total of approximately 26 options (brainstormed from a session of 15 people) from which the ESRT could select. The MSP seminar participants further evolved the identification of a number of potential scenarios, including some critical programmatic scheduling strategies that could be applied to the scenarios. Finally, the MSP seminar presented the factor of trade-offs. For example, a common rule of thumb for risk mitigation is 1:10; organizations should pay to mitigate those risks where the cost to mitigate is 10% of the cost if the risk becomes a problem. This

kind of reflective thinking about risk mitigation was a good example of executive mitigation possibilities.

As described in the MSP seminar, full mitigation plans include actions, milestones, contingency triggers and plans, identification of risk owners, and key measures to assess the progress of the plan and the changes in the risk itself. Also included are estimates of the scope of effort and cost accounting for the plan, as well as reporting mechanisms and charts, and clear identification of who receives reports, and how often.

5.2.3 Standardization of System Risk Management Methodologies[8]

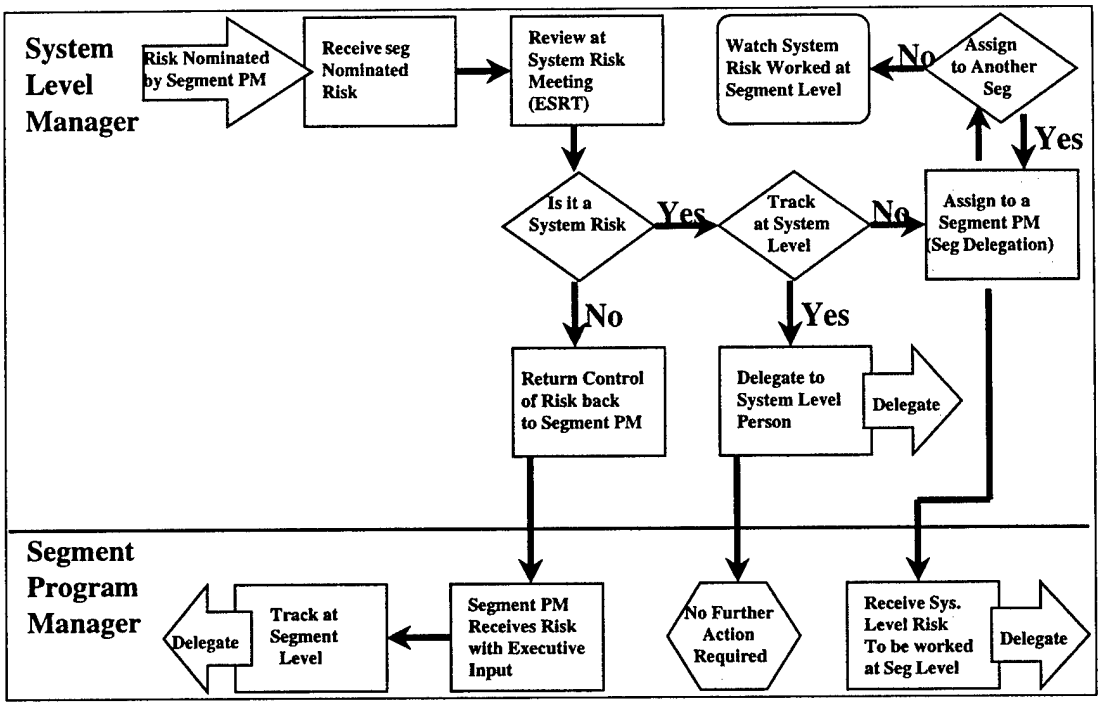
As mentioned above, the ESRT was, in many ways, slower to develop its own robust process than the divisions themselves were, due to the focused attention paid to divisional Risk Management capabilities and process installations. Therefore, for several processes, the ESRT was the last IDP Risk Management initiative to define and complete its rollout and installation process.

5.2.3.1 ESRT Risk Management Process

A regular meeting agenda was defined in December 1998. With this format in place, the ESRT proceeded to follow its process for surfacing, examining, and making decisions about system-level risks. In this process, most risks are identified first at the division level and are addressed within the division using its own process; if single divisional attention was insufficient to mitigate a divisional risk, or if a division believed there were wider impacts, a risk could be raised by a division to the ESRT. Risks could be identified directly at the IDP level because they derived from external sources or clearly had potential impact on several divisions. In addition, while most system-level risks were raised up from the divisions or identified by IDP management, anyone could identify a system-level risk if there was serious concern. The diagram below describes the high level Risk Management process at the system level.

[8] This section (5.3.4) contains excerpts from *A Guidebook for IDP Risk Management Practitioners*, by Pam Case and Jo Lee Loveland Link, © Carnegie Mellon University, 1999.

Figure 7: Standardization of Risk Management Methodologies



Graphic by Lenny Gentile, Oracle

5.2.3.2 System-Level Risks

The system-level risks addressed by the ESRT were those that

- have impact on program commitments
- have priority impact at the EIS system level on the
  - EIS program critical path
  - or any segment's critical path
  - or that exceed planned slack
  - or result in 0 or negative margin (those risks that seriously erode management reserve)
- have cost impact that exceeds planned budget
- make an impact on EIS interfaces, either internal or external to the program

5.2.3.3 System-Level Risk Attribute Criteria

When a new risk is entered into the system-level risk list, the ESRT will initially analyze the risk based on its established attribute criteria, as identified in the following table:

Table 4: System-Level Risk Attribute Value Table

Attribute	High/Near-term	Medium/Mid-term	Low/Far-term
Probability of Occurrence	70% < X ≤100%	30% < X ≤70%	0% < X ≤30%
Impact	Can't control vehicle OR can't perform mission	Can control vehicle, degraded mission	Can control vehicle, suboptimal mission performance
	Cost impact > $5M Schedule margin < 10% through launch	Cost impact $1M - $5M Schedule margin 10 – 15% through ship	Cost impact <$1M Schedule margin > 15% through ship
Timeframe	Less than 3 months out	3-12 months out	More than 12 months out

Based on this analysis, new risks are prioritized to determine the level of ESRT attention. As with divisions, the ESRT process follows the usual four options for managing risks:

- Watch the risk. Keep on the "screen" for review periodically for impact, potential loss, or the timeframe of concern, and any changes in these. "Watch-level" risks often have contingency triggers attached, so that if certain thresholds are exceeded, the risk is brought up for re-examination and possible action.
- Transfer the risk. If a risk is deemed to be one that can better be planned and managed by a division, or if it needs even more senior-level attention at the IMINT level, that risk is recommended for transfer. Even when a transfer is accepted, the ESRT may choose to retain that risk on its system-level risk list under the "watch" category.
- Develop a mitigation plan for the risk. Risks with significant potential impact and probability of occurrence will receive either a simple action plan or a more fully realized mitigation plan.
- Accept the risk. A risk worthy of identification but not within cost boundaries to mitigate is accepted, with action taken only if it becomes a problem.

On a regular basis, the ESRT reviews the system-level risks where attributes change, or other factors become important, such as additional cross-divisional impacts or program threats.

5.2.3.4 Standardized Data Formats

To accomplish their reviews with efficiency and broad system understanding, the ESRT standardized three specific data sheets, which were used by every division to capture, present, and track system-level risks: the risk information sheet, the stoplight chart, and the waterfall chart.

5.2.3.5 Risk Information Sheet

By late fall 1998, the ESRT had decided, by consensus, on a standardized risk information sheet. The format incorporated data fields from across divisions that division chiefs decided were important. While on the surface a simple-sounding document, this sheet was the first major consensus decision by the ESRT on "rules of engagement" after the EIS Risk Clinic. Agreement on the risk information sheet required that divisions relinquish idiosyncratic approaches, terms, and formats, and design a format that would be used for presentation of every system-level risk to the ESRT.

The risk information sheet is presented when a new risk is entered into the system-level risk list, and is available for all ESRT members to view electronically on the risk management tool, discussed below.[9]

5.2.3.6 Stoplight Chart

The stoplight chart is used at the ESRT to report the state of the mitigation plan for top division-level risks. *Green* on the chart indicates that a mitigation strategy is working as planned. *Yellow* indicates that the strategy is not working and alternative planning may be required. *Red* indicates that a mitigation plan has failed to mitigate a risk, and either a fresh look at the risk is needed, or the risk is no longer in the "probable" category and has become a current and full-fledged problem or issue that must now be managed accordingly—a "risk whose time has come."[10]

5.2.3.7 Waterfall Chart

The waterfall chart is used at the ESRT to describe progress in reducing risk exposure (the impact and probability factors) from *high* to *medium* to *low* for a single risk mitigation plan. The waterfall chart shows projected against actual progress, and indicates success or failure of the "buy-down" strategy being implemented.[11]

5.2.3.8 Tailored Division Practices and Information Displays

Section 5.4 describes the array of approaches and practices that divisions found useful for their own specific Risk Management processes. In addition, there were a number of practices used by divisions to analyze, plan, and track their division-level risks (fuller descriptions of these practices can be found in Section 5.4), including Segment 32's projection charts for schedule forecasting, and Segment 2's spreadsheet for tracking risks. These continue in use to meet division-specific information needs.

---

[9] See Appendix A.8, "Risk Information Sheet."
[10] See Appendix A.7, "Risk Stoplight Chart."
[11] See Appendix A.6, "Risk Waterfall Chart."

5.2.4 Risk Management Tool (RMT) Adopted as System Standard

By December 1998, the development and installation of the Segment 4 Risk Management tool (as identified in Section 5.2 and further discussed in Section 5.4.2.1) was showing promise as an interactive method to engage multiple divisional members in the active practice of Risk Management. At the same time, the RMT stimulated considerable user debate, and a requirements definition followed an iterative spiral-prototyping process.

By the beginning of 1999, the EIS program director had decided to incorporate the RMT as the standard electronic method for system-level Risk Management. All processes—from capture to analysis to mitigation plans to tracking—were to be leveraged through use by all divisions of the RMT for *system-level* risks. Divisional variations for internal Risk Management practices were left in place, though most members decided to move to the RMT for data capture and updates, for the sake of convenience, when a divisional risk might become a system-level risk, and vice versa.

Following the decision to migrate the RMT from one division's tool to the system-level standard, a robust process of tool assessment and modification began and extended over several months. As the RMT migrated from Segment 4/CCD to system-level application, the Development Systems Division took on ownership of ongoing RMT development. Tool developers from Oracle worked closely with the division's chief and staff to define the system-level interactive process, firm up the requirements, and complete the system-level RMT. Criteria for the RMT/system-level functionality included:

- configuring the system Risk Management tool to map directly to the system-standard risk information sheet, with consistent language throughout screens
- providing both a system and a divisional approach to risk exposure, so as to address the different specific attribute criteria at each level
- clearly identifying and appropriately leveraging authority to work risks based on management or divisional contributor roles; the ability to identify specific divisional teams
- improving ease of transportation among necessary Risk Management forms in the RMT
- incorporating into the RMT these necessary forms for system Risk Management reporting to the program director and upper IMINT and NRO management; the forms included the risk information sheet, waterfall chart, and stoplight chart

5.2.5 Interface of Risk Management with Technical and Business Management

As seen above, the EIS program director took seriously the importance of senior management "showing the way" to install as thoroughgoing a cultural change as Risk Management. The ESRT was established and announced as "the way system-level Risk Management will be conducted" in the initial meetings during spring 1998. Once the ESRT was operational on a

monthly basis, and the pilot program was increasingly proving the value of Risk Management to EIS senior management, the program director sought to further extend Risk Management into overall program operations.

As a result, the EIS program director identified three major meetings to "cover all the bases" and coordinate IDP program management:

1. Development Program Review (DPR), held monthly to review status of all projects and programs
2. Quarterly Program Review (QPR)
3. EIS System Risk Management Team (ESRT) meeting, held monthly to conduct system-level Risk Management

Over time, the ESRT developed improved processes to

- identify new system-level risks
- ensure analysis and mitigation strategy planning for risks, either through delegation to a task team, or by providing initial executive analysis/planning by the ESRT, as appropriate for the severity and complexity of the risks involved
- track and control system-level risks through review and revision of mitigation strategies when necessary
- communicate about critical path events, interdepencies, divisional interfaces, and other factors that could give rise to or provide improved mitigation strategies for system-level risks

Because these three meetings, in many ways, must be interrelated, program leadership has considered a number of reconfigurations. The critical factors here are

- how to fully integrate Risk Management into ongoing program and technical management
- how to retain a clear Risk Management discipline that resides within and generates from the divisions
- how to avoid losing the very real gains achieved at the system level by a proactive forecasting approach to the full program life cycle

Many of those at EIS who have become experienced at integrating Risk Management into their program management are convinced that looking ahead, as well as capable management, are jointly critical capabilities to ensure durable IMINT program achievement. IMINT continues to work to streamline and improve the effectiveness of information sharing and program planning and management. The system-level Risk Management plan has been signed by the system leadership; the RMT has been designated as the authorized system Risk Management approach to capture and manage system-level risks.

Where Risk Management is most mature in divisions, there has been a secondary positive support to program management. This support extends to improved streamlining and productivity of program/technical management forums and between-meetings work, and also provides actual results in program achievement and avoidance of risk consequences. (See "Success Stories" in Section 6.)

Still, integrating effective approaches to program management is an ongoing process. Best-practice approaches to incorporating Risk Management and program management continue to evolve at IMINT.

5.3 Divisional Risk Management Installations and Rollout of Risk Management

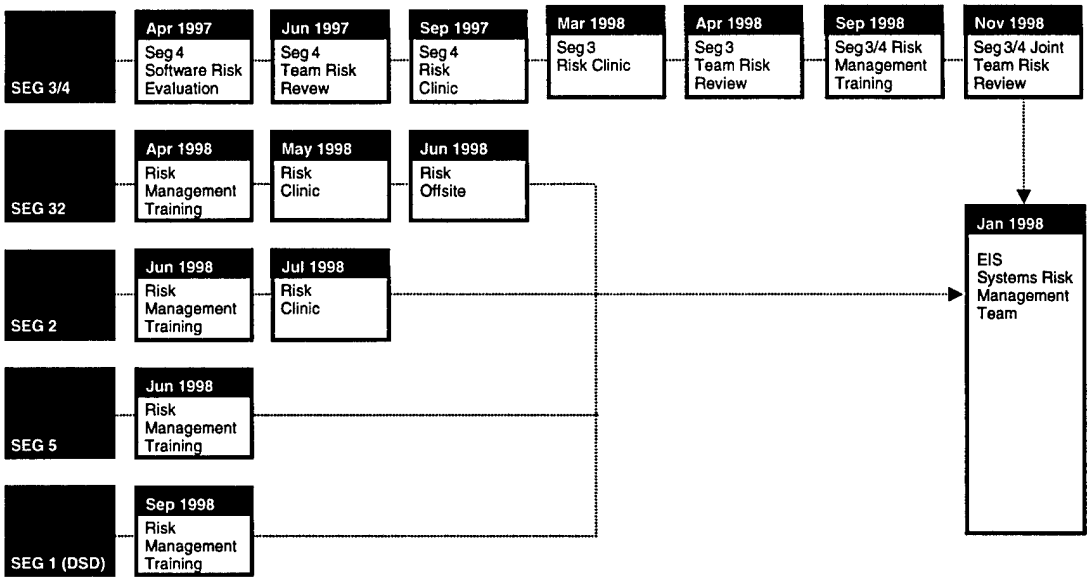
The previous sections described the pilot Risk Management program at IDP and the establishment of the ESRT. The next step taken by the EIS Program Director was to plan, together with the SEI project team, a divisional rollout across the system. The EIS Program Director recognized that a successful pilot and an established executive forum through the ESRT were critical but incomplete without full divisional installation. To achieve his goals for full system installation, the EIS Program Director further accepted that systemwide rollout and installation of Risk Management would entail a serious organizational commitment of time, training, and resources.

5.3.1 Overall Plan for Risk Management Training, Risk Clinics, and Risk Management Processes in IDP Divisions

The plan that the Program Director decided to launch included

- a series of Risk Management training sessions for each division
- Risk Clinics where divisions decided they would be helpful
- installation of a division-tailored Risk Management process in each division
- "bubbling up" from each divisional risk list those risks with system-level impact to the ESRT for management team consideration and action

Figure 8: Divisional Rollout and Installation



5.3.1.1 Key Success Factors in IDP Risk Management Rollout and Installation

The program director adopted the key success factors in successful Risk Management rollout and installation as guidance for this rollout and installation. These success factors included

- an overall plan and process flow with steps for rollout and installation in each division
- alignment with cultural considerations, including the system's history of improvements, as well as the level of readiness and skepticism in the system. In having the Risk Management course tailored for IDP divisions, and deciding to allow for tailoring of the Risk Management process among the divisions, the program director paid heed to the existing culture and effective approaches that already existed, or were developed, among divisions.
- division input into the system-level IDP Risk Management plan—the full plan to guide the system-level Risk Management process
- integration with existing business and technical activities, including existing meetings, critical path priorities, and program goals
- and the key success factor, committed leadership

5.3.1.2 The Critical Success Factor: Committed Leadership

As was pointed out in Section 5.3, IDP was fortunate to have a series of highly committed, knowledgeable leaders who were themselves interested in mastering Risk Management. In particular the initial IMINT and IDP planners who worked with the SEI on Risk Management included a succession of senior IDP leaders who have shown their commitment to Risk Management through willingness to commit serious resources for installation of the Risk Management process. Not only were they ready to focus priority attention on Risk Management

and devote the necessary resources; they were willing to take the critical, very visible public stands that showed the organization that they were serious about Risk Management.

In any organization, improvement and new practices are seen as "extra work" until proven. Paradoxically, new practices such as Risk Management cannot prove themselves until initial investments are made and installation has been functional for some time. Even where early successes are widely acknowledged by system members, there are always a few times during the rollout process when the "going gets tough." It is natural for people to become tired and frustrated sometimes. This is where the committed EIS system-level leadership especially helped the organization keep on course—through repeated messages, focused attention, and other visible support for Risk Management.

5.3.1.3 Plan for IMINT Risk Management Training and Clinics

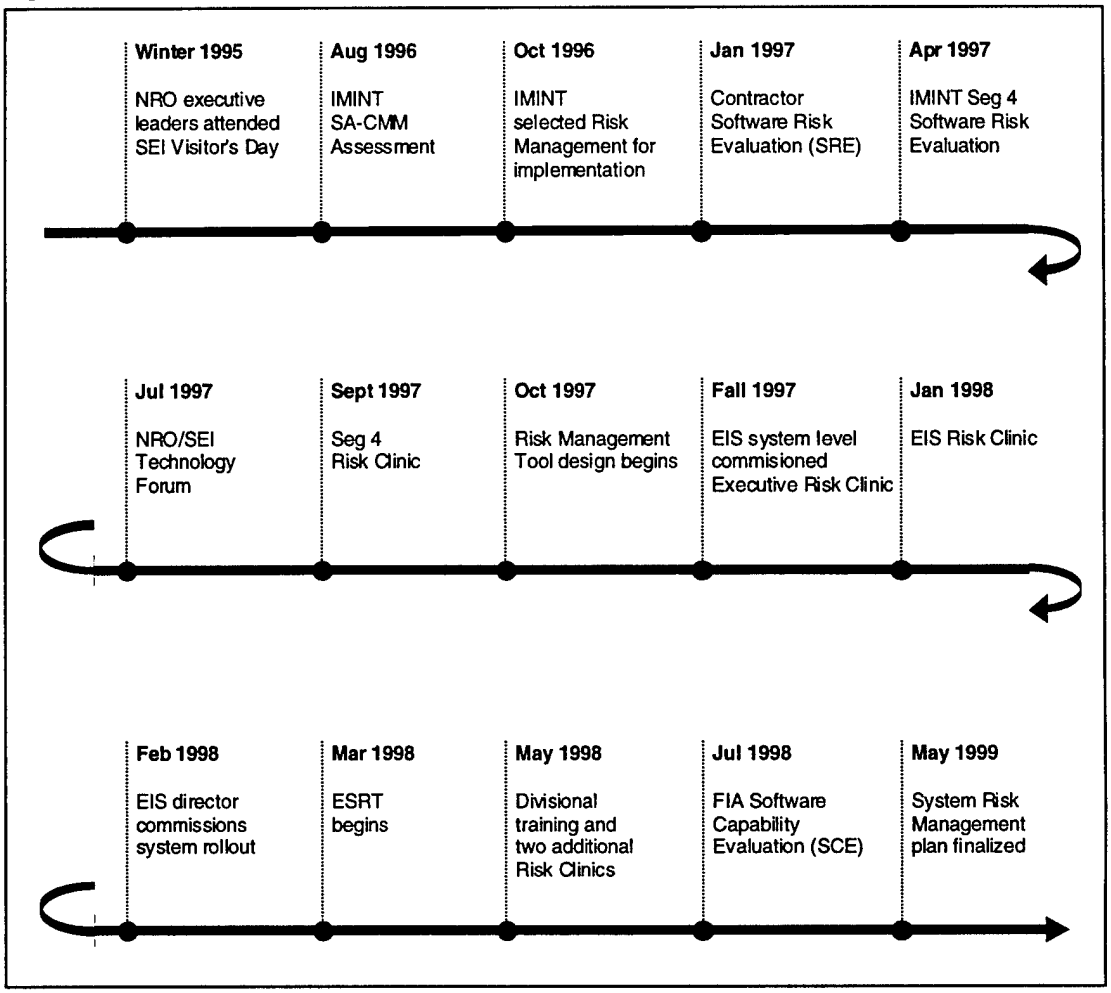
Understanding that there was a need for significant investment in development of knowledge and skills for IDP Risk Management to be successful, IDP Director Al Krum mandated Risk Management training for every IDP division. He further mandated that SEI tailor its three-day public Continuous Risk Management Course into a two-day modified version for IDP, and that the course should be named the "IDP Risk Management Course" to differentiate it from the "outside" version. He also directed that the course focus on in-class discussion and examples that addressed NRO-, IMINT-, and IDP-specific issues and concerns. Finally, he set a timeframe for delivery of all training sessions to conclude within six months from the initial training session, and for each training session to be followed by divisional risk clinics where divisions requested them.

Concurring with this guidance, SEI tailored the IDP Risk Management Course and conducted sessions with all five IDP divisions. In addition to the system-level Risk Clinic that led to formation of the ESRT, three of the divisions requested Risk Clinics of their own, which were conducted as well.

5.3.1.4 Risk Management Rollout and Installation "Events Map"

All training and Risk Clinic delivery activities were completed in the seven months between March and September 1998. The broader schedule for Risk Management rollout and installation extends beyond these dates and includes the SA-CMM assessment, the Segment 4 pilot Risk Management effort, and the establishment of the ESRT. The total timeframe for rollout and installation of Risk Management at IDP, including these activities, began in January 1997 and was essentially established by June 1999. The "events map" for the overall project, including the SA-CMM, the pilot effort, establishment of the ESRT, and divisional rollout and installation, and other key events, is as follows:

Figure 9: Overall IDP Risk Management Rollout and Installation Events Map



Note that this events map is predicated on the regular coaching and facilitation that are essential throughout the rollout and installation processes, and must be ongoing for a time to ensure successful installation of robust Risk Management. These activities are integral to the SEI system-wide rollout and installation process of Risk Management. Therefore, targeted and vital support for Risk Management activities must be part of any planning for further dissemination of Risk Management across the NRO.

5.3.1.5 Implications for Downstream Risk Management and New Installations

As a result of the entire portfolio of cumulative IMINT Risk Management course deliveries, Risk Clinics, coaching and facilitation activities, "brown bag" presentations for the Acquisition Center of Excellence, presentations on the entire SA-CMM for IMINT-wide audiences, and two briefings for the Acquisition Steering Group on the Risk Management tool, there was a considerable increase in the number of people across the organization who were knowledgeable about Risk Management.

One impact of this growing organizational knowledge was that each successive divisional Risk Management training experience was richer in substance, and required less description of Risk Management mechanics. Meeting briefings that include informal "hallway talk," substantive discussions with Risk Management experts from the SEI and inside the system, and other opportunities for learning have all contributed to a growing body of knowledge on Risk Management throughout the organization.

The organization's increasing level of sophistication means that further tailoring of the IMINT Risk Management training courses and materials is recommended for future deliveries. In addition, there was widespread conviction that integration of at least a high-level risk identification session, along with the Risk Clinic, would be optimum for the rapid launch of Risk Management across the organization.

An additional forewarning: as people become more knowledgeable, misconceptions and misunderstandings can spread. Caution must be taken to ensure that the core messages and knowledge base are integrated and consistent. Optimum leverage of knowledge requires vigilance.

5.3.2 Tailored Variations in Risk Management Among Divisions

Some people who are new to Risk Management are concerned that constraints will be imposed on their operations from a "one-size-fits-all" Risk Management practice. Others may believe that there is "one right way" to practice successful Risk Management.

While it could be argued that the NRO, IMINT, and IDP are really all one system, the IDP Risk Management installation alone provides good insight into a system-wide installation because it displays a wide range of local variations in actual practice among divisions. As such, the experiences at IDP can reassure newly engaged Risk Management practitioners—at NRO and elsewhere—that there are rich possibilities for tailoring installation to an organization's specific and unique needs and existing infrastructure.

As shown in the earlier discussion, a number of key success factors for successful installation of system-level Risk Management. For a system-level Risk Management process to operate effectively, there must be standardized formats and templates for efficiently sharing information on risk (such as an integrated risk information sheet and meeting presentation templates). There also must be an established system-level infrastructure for regular management discussion, problem solving, and planning with regard to risk interfaces.

However, it is important to note that local variations are not only acceptable but are the lifeblood of successful Risk Management practice. Each division may—while integrating the essential functions of Risk Management into how they do business—have Risk Management processes that look very different. For system-level integrated efforts, divisional leaders can

and should create together, by consensus, the system-level Risk Management processes, and the practices and methodologies to support them.

At IDP, as we have seen, all four primary technical divisions as well as the System Integrator Division participated in the IDP Risk Management Course. Only three of the five divisions, however, conducted a Risk Clinic to build their Risk Management process from the ground up, though the executive team also conducted a system-level Risk Clinic to build an integrated Risk Management process that would tie everything together.

By their own reports as well as those of other divisions, all three of the divisions that conducted a Risk Clinic and launched their own internal Risk Management process reaped some dividends from integrating those processes into their business operations.

And, while candid, open, and shared communication is a key success factor, it does *not* require an "open-systems" management style—contrary to some expectations. The preferred and comfortable style for each division differed a great deal; a top-down, chief-driven Risk Management process appears to work as well as a more participatory style. On the other hand, as divisions progress in their Risk Management process and become more sophisticated risk managers, division chiefs seem to become more comfortable with delegating a greater "front-end" portion of risk identification, analysis, and prioritization to their staffs.

In fact, in the divisions practicing active Risk Management, there is a spectrum in relation to government/contractor partnerships on joint risks and shared Risk Management. This ranges from a distant, "arms-length" Risk Management approach (with one process being used on the government side, and a different one on the contractor side), to an active Team Risk Review (TRR), which is the Integrated Process Team infrastructure recommended by the SEI. The system-level Risk Management team, the ESRT, consists of members drawn from both divisional leaders and from contractors involved in system-level work.

Following is a description of the Risk Management processes for each of the five divisions.

5.3.2.1 Segment 4 Risk Management

Segment 4 was the Risk Management pilot site for IDP. As such, the specific organizational events that contributed to this division's rollout and installation have been largely described in Section 5.1.

This section will describe the experiences and perspectives of the key individuals involved, in particular the area manager who championed Risk Management for the division, Tommy Meeker, and the division chief, Gus Neitzel, as Risk Management was introduced and installed in Segment 4.

The groundwork for introduction of Risk Management was laid as a result of a 1995 Malcolm Baldrige National Quality Award assessment of the NRO, conducted shortly after

the merger of certain operations of the Air Force and the CIA into one unified mission organization. Based on the testimony of both Baldrige and organizational spokespeople, this merger inevitably clashed two dissimilar cultures and ways of doing business, a dynamic that persists today. Also during this period, Congress mandated the establishment of the Enhanced Imagery System, coupled with a directive that the NRO become more efficient and effective. These two events spurred IMINT leadership to seriously consider the SA-CMM assessment, and to select Risk Management as the initial SA-CMM key process area to install.

The SA-CMM assessment found that several Level 2 process areas were satisfied, at least in part. The Level 3 Risk Management area was a glaring omission, both as a government practice, and as a process area of contractors that the government understood how to manage.

As a result of these findings, IMINT leadership decided to go forward with the Software Risk Evaluation, and selected Segment 4 as the pilot for assessment. The Segment 4 division chief has candidly described elsewhere his initial reactions to serving as the pilot.[12] (IDP and IMINT leadership indicated that they believed Segment 4 would be a valid test site.

As Risk Management installation began, Segment 4 reduced the initial 77 risks to 10 affinity groups. Then, reasoning that they "couldn't do everything," Segment 4 selected four of those groups on which to focus. The division performed mitigation strategy planning on these, developed an initial database, and launched a government/contractor Team Risk Review (TRR)—but without the benefit of a Risk Clinic, a decision which several Segment 4 members, including the division chief and his area manager most involved with Risk Management, later cited as a "serious mistake."

According to the area manager, Segment 4's first exposure to the SEI approach to Risk Management was at the 1997 Risk Management Conference, "Managing Uncertainty in a Changing World," held April 7–9, 1999, in Virginia Beach. The NRO participants "found high value in the Risk Management approach they saw there," the manager said.

However, after the startup phases of Risk Management, some Segment 4 principals began to have serious doubts about the installation's value, which could be summed up in the following comment: "We were not interested in learning a new vocabulary—if Risk Management could not help me get my job done every day and provide value-added, then we were not interested." By "value-added" members meant "cost-efficiencies, better scheduling, and technological capability, as well as the extra dimension of taking the organization to the next level of performance." IDP senior management reinforced that the choice to engage in Risk Management was Segment 4's, and that there was no coercion from above that would require them to participate.

As a result, Segment 4 and IDP leaders met with SEI staff members to discuss the growing dissatisfaction in Segment 4 with the Risk Management process. During that meeting, both

[12] See Appendix A.1 "Managing Risk Management," by August C. Neitzel, Jr.

IDP and SEI members identified areas where they perceived obstacles to an effective working partnership. Division members described their requirement of value in terms of improved performance of their actual operations, and SEI staff members identified the "missing link" in Segment 4's Risk Management installation, the Risk Clinic. As a result of this candid discussion, a new agreement for honest interaction and joint commitment emerged. The Segment 4/SEI partnership was forged, and all parties expressed a commitment to "make it work."

5.3.2.1.1 Segment 4 Risk Clinic

The Risk Clinic was the final persuasive evidence for Segment 4 that the process could actually help improve the way they did business. As the area manager said, "We saw engineering being applied to the process, and we built a 'flight plan' that would work, and that we knew we could modify when appropriate." This last aspect was very important for this divisional team.

As an outcome of the Risk Clinic, the Segment 4 Risk Management plan has steered the division's process, and has been adapted over time to reflect changing practice. The Segment 4 plan has also served as an example for other divisions to consider when tailoring their own process preferences. It has been emphasized at every point that the Segment 4 plan is not a "model plan" but rather an example of only one approach. The plan has been tailored to provide optimum utility for each division; however, the original plan has been a useful "launching pad" for others to examine.

According to the division chief, there were at least two important outcomes of the Risk Clinic:

1. The entire Segment 4 team, government and contractors, "got the language straight" to communicate effectively about risks.
2. Previously, the procedure was to delegate Risk Management to the contractor (and Segment 4 still counts on the contractor for mitigation, as the government has limited resources for this activity). However, with the monthly TRR, the government accepted ownership of program Risk Management, and government/contractor teamwork has become genuine. The TRR provides management perspective, political experience, technical expertise, and financial insight, all working together on the same team. This was a totally new experience at IDP.

5.3.2.1.2 Established Segment 4 Risk Management Process

After the Risk Clinic resulted in a plan to guide the Risk Management process, the regular TRR became a constructive and candid meeting. Nevertheless, as previously discussed, even after the establishment of a regular TRR and the area manager's "Starbucks" meetings, there were some newcomers to Segment 4, as well as the entire staff of Segment 3 (see discussion below), who had not experienced either the Software Risk Evaluation and its associated activities or the Segment 4 Risk Clinic. A Segment 3/4 IDP Risk Management training session was scheduled in September 1998.

This session was attended not only by Segments 3 and 4 (including some participants from the above-named Risk Management events) but also by the Segment 4 contractors, who participated in force, including both senior managers from the key programs. A full discussion of the outcomes *for the contractor* is below; for Segments 3 and 4, the results were increased clarity about the Risk Management process, an enhanced common language, and an expanded government team commitment to Risk Management.

The TRR continues to be the cornerstone for Segment 4 Risk Management. Indeed, both government and contractor have had several opportunities to evaluate whether the TRR should reduce its meeting schedule from monthly to less frequently. The consensus to date has been not only that the TRRs should continue as before but that "this is the only meeting where we really get a chance to talk with each other and problem-solve honestly" and that "losing the TRR would be a real loss for our program and its ability to be successful." Comments such as these have been made by both government and contractor members of the Segment 4 TRR.

Current interest in Risk Management in Segment 4 has led to new explorations. Due in part to its advanced stage of development (having started as the pilot) and in part to an interest in expanding its Risk Management capability even further, Segment 4 has been working on the development of a schematic for Risk Management earned value and a system of risk metrics.

5.3.2.1.3 Segment 3 Risk Management

Segment 3 primarily involves a hardware development effort. Of the eight major subsystems in the segment upgrade program, only one, the Control and Status Subsystem, is software-oriented. The remaining hardware subsystems are complex and contain extensive embedded firmware, particularly in the Wideband Data Subsystem. The introduction of the IDP Risk Management approach and its integration with the legacy Risk Management procedures used by the contractor demonstrated the applicability of formal Risk Management—proactive identification and mitigation of risks—for this hardware-oriented program as well as the software-oriented work of Segment 4.

The Segment 3 upgrade acquisition has been managed from the start using formal integrated product team (IPT) procedures, which continue for the life of the development contract. A formal risk identification and management system was in place by the contractor prior to integration with the IDP and Segment 4 Risk Management process. However, the government did not have its own Risk Management process, nor was there a jointly managed process. Prior to installation of the government Risk Management process, the contractor was already providing briefs on its risks at the Segment 3 monthly Program Management Reviews (PMRs).

In March 1998, Segment 3 underwent its own Risk Clinic, with participation by government and contractors. Immediately following the clinic, the first joint contractor/program office

joint risk list was developed. This was followed by the startup Segment 3 Team Risk Review (TRR) on April 15, 1998, and included the three Segment 3 IPT teams: government, system engineering/technical assistance (SETA contractors), and the development contractors. In this initial session of the monthly Segment 3 Team Risk Review, procedural outlines were developed, and by June 1999, the Segment 3 Risk Management Plan, TRR membership charter, and TRR process flowchart were completed. These remained in working draft form pending resolution of the EIS System Risk Management plan and the system Risk Management tool.

The Segment 3 Risk Management plan was aligned with the Segment 4 plan, especially regarding the attribute criteria for establishing the impact, probability, and timeframe for each risk. Segment 3 added to the Segment 4 criteria a cost-exposure factor to closely manage program costs and contingency reserves.

An important tool used by Segment 3 to surface risks was analysis of its technical performance measures (TPMs), which are key, quantifiable system- or product-specific performance metrics. TPMs, defined early in the program prior to the critical design review (CDR), assessed how well the product performs its functions (i.e., acquisition time, BER, transmit spurs, and directive execution time). TPMs provided visibility into actual vs. planned performance, with the benefit of early detection or prediction of technical challenges that would require management attention. Close monitoring and reporting of the TPMs to the COTR in PMRs provided a valuable tool to surface risks.

Prior to each monthly TRR, the Segment 3 TRR facilitator prepared a draft package of all risk updates as well as candidate risks for TRR consideration. During the formal TRRs—usually conducted in conjunction with the monthly PMRs—the context, mitigation plans, and probability impact assessments for each risk were reviewed.

The TRR joint risk list was established using multi-voting techniques in which the three Segment 3 government/contractor teams each evaluated a risk by assigning weighted values. The sum of the assigned weights from each of the three teams determined the relative ranking of the risks. Any ties were resolved by the TRR lead. A review of the history of the TRR joint risk list multi-voting shows remarkable consistency among the evaluations from the three groups over a span of 15 sessions; however, the TRR procedures allowed for and encouraged open discussion on divergent issues when necessary.

Results of each TRR were formally documented and distributed in minutes to team members.

This more robust joint government/contractor Risk Management process—whereby risk exposure was quantitatively evaluated on a continuous basis—has proved extremely valuable in identifying, quantifying, and mitigating program risks.

In addition to its own TRR, Segment 3 participated in the Segment 4 TRRs to optimize program Risk Management coordination and shared knowledge of risks. In November 1998,

with the completion of its critical tasks, Segment 3 moved to the Segment 4 TRR for all of its TRR activities.

5.3.2.1.3.1 Success Story from Segment 3

Among several program breakthroughs associated with government/contractor Risk Management, Segment 3 was successful in obtaining some new resources because of its risk identification, analysis, and mitigation of the risk of losing critical skills. Joint analysis and discussion by the government and contractors in the TRR provided clarification with specific data on the investment-versus-payback for this risk. The analysis was coupled with inventive, jointly derived strategies to support mitigation of the loss of critical skills. This risk, and its accompanying mitigation strategies and quantified analysis were passed "up the chain" to senior management.

5.3.2.1.4 Initial Development of the Risk Management Tool for Segment 4 Risk Management

Discovering that few commercial off-the-shelf products existed to enhance practices at the level of Segment 4 Risk Management, the area manager coordinated a technical team to create a tailored Risk Management tool that would automate some processes and foster daily Risk Management interactions electronically among Segment 4 team members. A risk to the Risk Management process itself was identified: knowledge management atrophied between the monthly TRR meetings.

The goals of the Risk Management tool (RMT) initially were to

- get everyone thinking regularly about Risk Management
- build an online, leveraged conversation among team members, so that everyone could communicate in a soft-copy environment
- provide the division chief with timely, analyzed information about current and potential risks in the division
- establish a rich database that could be accessed easily and through which risks could be analyzed in a number of different, useful ways
- provide a tool that was not just a relational database, but was interactive and provided valuable management decision-making information

There were some difficulties with the RMT. The original engineering version was less than user-friendly. Also, because of NRO technological changeovers and differing platforms, the RMT was not available on everyone's desktop. And, initially the division chief had the only master copy of the Segment 4 risk list. All these issues were eventually resolved and, as described elsewhere, the RMT was adapted for system-level use to incorporate all divisional risk inputs.

The benefits provided by use of the RMT include "forcing the team to think about Risk Management, and to think *together* as a team," in the words of one manager. The RMT has become a user-friendly tool and rewards people who use it with improved data and interaction on Risk Management.

Despite the RMT's current and increasing benefits, the area manager who led the way in building the RMT emphasizes: "The tool, without the Risk Management process, is meaningless. The tool leverages the process; it does not replace it." Indeed, to expand on vital and current information, this area manager established Monday morning "Starbucks meetings" for all Segment 4 area managers. These were stand-up meetings specifically designed to be brief, as well as to create a regular forum to identify potential new risks, track mitigation plan effectiveness, and consider alternatives when necessary.

5.3.2.1.5 Government/Contractor Risk Management Relationship at CCD

As outlined in the section on Team Risk Management, the government/contractor partnership is the heart of a successful team approach to achieving program results. At CCD, the pilot organization, Team Risk Management was established and leveraged through monthly Team Risk Reviews. However, as seen in the discussion on development of the pilot program, development of this relationship was not instantaneous or easy. As with many Risk Management practices, there is no "silver bullet" for building a sturdy, creative, effective government/contractor relationship. As is common, the government and contractor members of the CCD TRR found that forging the shared product/program vision that is required for Team Risk Management challenged individual preconceptions of the "rightness" of "my" perspective for many team members. To create a successful government/contractor partnership, these challenges had to be overcome, and were successfully surmounted by the CCD TRR.

The TRR partnership at CCD, as verified by both the government and contractor, has matured into a vibrant and durable one, though the original Team Risk Review formation was challenging for both sides. The groundwork for mutual trust and confidence grew through putting on the table honest differences of opinion and goals and working them out. The CCD government/contractor team jointly negotiated the TRR purpose, goals, operating guidance, and Risk Management approaches to mesh their separate perspectives into a team with a common understanding and commitment to mission success.

"A plan that does not include management reserve and schedule slack is not a plan, it's a wish," was the perspective of Kevin Wardlow, a contractor manager for CCD. "It's only wrong to be wrong when you don't leave room to be wrong."

The "biggest obstacle to Risk Management," said Milt Harrison, another contractor manager for CCD, is this: "Are you willing to share your risks? This may sound simple, but it is the core question. Risk Management cannot succeed in a 'penalty situation.' "

The CCD TRR included participants from both development and follow-on contractors. Both contractor organizations established Risk Management processes that were supportive of the government and applied the following:

- The contractors redesigned their Risk Management processes to align with the government team's process following the joint Risk Management workshop.
- The follow-on contractor developed a comprehensive set of standard operating procedures (SOPs) to govern its risk and issues-management process. The SOPs included a team charter, a defined Risk Management process, clearly specified roles and decision authorities, approaches for risk mitigation, and other pertinent information. The SOP served as an ongoing reference for the contractor team, as well as an orientation handbook for new contractor staff.
- In addition to cost, schedule, and technical risks, the contractor included "management risks" defined as "risks that internal structures and decisions will drive risk in the other three risk areas and/or will have negative impact on the business parameters of the program"—a value-added parameter often ignored in Risk Management.
- The contractor held a weekly "risks and issues" meeting at which attendees surfaced new risks, devised mitigation plans, established "red flag" triggers for mitigation actions, and developed quantifiable workoff plans complete with milestones and measures of success.
- In November/December 1998—because of a number of events, including a significant replan activity, changes to cost/schedule/risk baseline, and identified gaps in the current Risk Management processes as a result of the IDP Risk Management training—the development contractor conducted a risk-taxonomy review to ascertain whether any previously unfound risks had emerged since the SRE. With a number of "lessons learned" on value from the taxonomy (see below), the contractor proceeded with a renewed confidence in its portfolio of risks and a reinvigoration of its Risk Management process.

Lessons learned from the contractor's risk-taxonomy review concluded:

- Taxonomy review is appropriate to verify risks during times of major baseline change.
- A periodic taxonomy review encourages "the troops" to "think collectively about the big picture."
- The taxonomy review does not replace the need for gathering risks on an ongoing basis.
- Using the right forms and thorough analysis (including, importantly, context as well as risk statements) during the taxonomy review "forces completion of the risk analysis" so that "you are ready to roll with risk mitigation."
- Basic "block and tackle" includes choosing the right leader—someone who is "process knowledgeable, visionary, organized, a superb facilitator, not mired in program concerns, and dedicated to the initiative with a firm timeline."
- It is important to prioritize the activity and motivate the team.
- Group discussions "can be very effective if buy-in and cross-organization participation are there."

The results and rewards of the taxonomy review did not so much identify surprises. Rather, the contractor team validated its own open-communication channels, and did discover some innovations in how certain risks could be combined and more productively mitigated and assigned ownership for resolution. There was also an assurance for the contractor team and its management that "no surprises" meant that they were unlikely to encounter unplanned challenges, and therefore could focus on the "tough, high-attribute risks" that required close mitigation, tracking, and action.

5.3.2.1.5.1 Knowledge Management as a Core Concept for the TRR

The follow-on contractor-manager introduced the concept of "knowledge management" to the TRR. The follow-on contractor has commented, "The TRR transforms basic data into usable information, which can, with the right discussion, leverage into knowledge for critical Risk Management plans and execution. Knowledge resides in people and therefore—without effective interaction of the people—risks cannot be managed effectively. Knowledge applied in Risk Management creates bridges across people in the organizations—knowledge resident in the minds of each contributor is integrated to achieve solutions that work, since it is derived from a range of thought not possible in one person's mind alone."

The concept of knowledge management was adopted by the TRR as a value-added way to describe the kind of intensity and depth of discussion that actually takes place in this Risk Management forum. The TRR is unlike "status" meetings, or staff-action meetings, or other sessions where speed and firm data are transmitted. As confirmed by the development contractor, the TRR provides a space where participants can "talk with confidence of respectful listening, as well as discussion of different views. Nobody dismisses other ideas as 'unworthy.' People 'take off their uniforms' and their organizational roles, and turn their attention to what is best for the program. We can openly discuss the real risks of not making schedule, and engage in full, out-of-the-box discussions about how to work together to mitigate those risks."[13]

5.3.2.1.5.2 The Value of the TRR Government/Contractor Partnership from the Perspective of the Contractor

Building on the perspective of knowledge management, the CCD TRR has institutionalized a forum where issues are responsibly and openly raised. Over two and a half years of regular meetings of the TRR, the candor and open discussion necessary to achieve Risk Management have continued to expand. By June 1999, the government and contractors had achieved high performance in the TRR, which was revealed in significant breakthroughs and successes in Risk Management, both in their separate efforts and together.

---

[13] For a further discussion of knowledge management, see Chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

The TRR is formulated as a "working session," which means that ample time is provided for discussions for the evolution of data and ideas to become useful information and knowledge. Both government and contractor managers reinforce the value of the TRR as the "one meeting where open discussion can occur" and where, as one contractor manager said, "positions and hierarchical levels do not get in the way of candor." Everyone in the TRR understands that the government division chief is "where the buck stops," but the value of exploring risks, and even broader issues, has proven itself to the managers and other participants in the TRR. The TRR has grown to provide an environment where, as described by the development program contractor, "we are able to accept the fact that no one of us has all the answers—and we don't need to. We can now expose situations where we *don't* know the answers, and trust that someone else will. The TRR works because one person may be astute in perceiving a risk, but not know how to fix it; another may have the domain expertise to provide a good solution."

Elsewhere in this report, government perspectives on the value of Risk Management and the TRR specifically have been addressed; for the other half of the story, the CCD contractors provided their insights as to the value of their Risk Management partnership.

The CCD contractors identified a number of specific value-added contributions that the TRR has provided to the government/contractor partnership:

- Team Risk Management transforms vague concerns to specific plans, worry to action, individual opinion to joint criteria for decisionmaking.
- Team Risk Reviews achieve better program results, propelled by common agreement on the vision of program success through closely-integrated joint team efforts.
- Knowledge management inherent in the Team Risk Review process benefits greatly from the diverse assets represented in the joint government/contractor, multi-level TRR membership: the sum is larger than the parts—ideas and concerns are often presented in various forums, including off-duty time. Having "multiple receivers" for this informal information enriches the Risk Management process.
- Contractors were at liberty to speak up in the best interests of the program, actually recommending several times against courses of action that would lead to more expensive "buy-by-the-drink" approaches.
- Contractors at the TRR also reported gaining better insight into the issues and pressures faced by their government counterpart. This in turn allowed the contractors to serve as better partners.
- TRRs benefit from adding new members with new information to refresh the knowledge base (though new members require guidance for their learning curve on Risk Management).
- The TRR drives understanding of risks, which in turn drives understanding of what needs to be done about the risks, so progress can be measured against desired outcomes.
- If Risk Management is set up right, all stakeholders will be aware of what risks and mitigation plans are in place and, if the right people are involved, there will be a stronger team execution of mitigation actions.

- The value of mature Risk Management spreads beyond the Risk Management forums themselves; once people start to think proactively, it benefits all aspects of program management.
- The bottom line: the TRR is successful because it is built on trust, provides face-to-face discussion on serious issues, and assures a non-penalty environment.

The contractors also provided some lessons-learned and reminders:

- Even in an atmosphere of openness in the TRR, participants are sometimes reluctant to speak up and their contributions may need to be solicited.
- Periodically, who attends the TRR and for what purposes may need to be revisited. "Be careful of the 'gallery,' said one contractor. "It takes time to build the kind of trust and candor that we have achieved. The right people need to be there; onlookers should be discouraged."
- Respect for proprietary considerations for contractors—especially in a multi-contractor TRR—may need to be reinforced.
- Leaders need to take Risk Management seriously as integral to the way they run programs; if staff are asked to provide a one-chart summary of their program, and Risk Management is not on that page, chances are it's not being done, and the leader needs to find out why and make sure of enactment in the future.
- Having risks is a sign of program strength—the opposite of what people new to Risk Management often think. A program should not be considered a failure because it has risks. Having no risks means either (1) you have a simple program or (2) you're not managing well. People should not be afraid to go up the chain and own up to risks—get rid of the "shoot-the-messenger" syndrome.
- Remember that the TRR is "not a status session," as one contractor pointed out. "The agenda needs to be formulated, but should contain enough flexibility that the 'unknown unknowns' can be explored. Charts do not need to be as polished as those for a formal review. The focus needs to be on the quality of the discussion, rather than speed and presentation."

The contractors reported that overall benefits from a joint Risk Management process were more pervasive than the TRR itself. The level of open discussion created benefits outside the TRR. The monthly contractor system review was transformed from a meeting with considerable separation between government and contractor to a discussion in which the only liability was a failure to disclose risks.

The development contractor pointed to the fact that a closer partnership with the CCD division chief benefited the "balancing act" that must be done in leveraging end-user concerns. Being able to discuss risks openly with the government manager as the "gateway" to the end users assured both better communication and respect for issues of scope.

Finally, in the words of the development program contractor, "As a result of the level of honesty and trust established in the TRR, (the contractors) were able to communicate clearly to the CCD division chief our commitment to the program—that we will not allow him to fail."

5.3.2.1.5.3 Success Stories from the Contractors

The contractor organizations pay close attention to rapid response to crises, while maintaining a long view to capture lessons into a "virtual organization" library. The organization communicates its knowledge assets via a Web page that provides continuous improvement as well as current project/task information. As each project is brought to closure, there is in the project plan a trigger to conduct "lessons learned" reviews. When the project team's proposed lessons are compiled, they are sent to a review board and a judgment is made on whether they are durable lessons to include in the knowledge assets repository.

When necessary, this process can be managed very quickly for project lessons with broad system implications; a recent correction was completed in 24 hours, and the "lessons learned" package was sent out immediately to help reduce recurrences in other projects right away. This process leverages Risk Management through this almost instantaneous transmission of critical project improvements.

The contractor Risk Management process also acknowledges that human error is inevitable—"there may be nothing wrong with the plan, the project, the technical design, etc.," said one contractor manager, "we still have to be alert to the inevitable human errors. We 'harden the system' to human error by integrating performance monitors and verifications at regular checkpoints."

Within this context of risk alertness, there have been a number of success stories that the contractors saw as attributable to the strengthened government/contractor partnership, which were:

1. Hitting the SCR-TE 1 schedule date. Risk Management provided simplification for development, which assured that the program reached the target date (against widespread expectations that it would not be made).
2. Improving CCD critical skills: The combined forces and best thinking of government and contractor were marshaled to resolve the issue of Segment 3 critical skills. The follow-on contractors built a diagram that showed the *quantified* impact of the loss of critical skills on system availability over time, which calculated the mean time between failure breaks, figured in lag times as well as specific system parts that could break, and their further impact.
3. The follow-on program was responsible for converting mainframe-hosted engineering software to the distributed system. Given schedule constraints and associated risks, the contractor redesigned the system architecture platform so that tools could not only function in the new environment, but some software could be left on the mainframe to save time and effort in rewriting and conversion, and focus on the interfaces created.

To accomplish this, the contractors defined the risks involved, examined alternative mitigation strategies, including thinking through what would happen if they stopped the conversion process and worked the interface at given points in the development. To build a solution, they designed prototype plans to prove concept, measured observables to gauge success potential, analyzed the schedule against the critical path, and identified a "point-of-no-return" contingency trigger date. All risk planning was completed in a week and a half. As a result, 20 of 30 applications were saved, in addition to more than 50% of the originally planned effort.

The successes here were multiple: improved schedule, reuse, time, and skills released for other pressing needs.

4. Delivery #1 Transition: the contractor risk mitigation was the entire transition plan. To accomplish the transition, they began by asking key questions, such as: Provided Delivery #1 was transitioned successfully, what would happen if the contractor was not ready? What would "ready" look like?

   To mitigate this portfolio of risks, the contractors reviewed a robust view of the risk taxonomy, including technical review, program management, and maintenance. Over a two-month period, they wrote a 100-page plan with 47 identifiable tasks, individual assignments, and due dates which were statused weekly. As a result, when transition occurred, technical readiness was in place. With no perturbations, the change of ownership was seamless and invisible to anyone outside the process.

5.3.2.1.5.4 Team Risk Reviews and Parallels with IPTs

Building a true team of any kind is difficult. Research on integrated product/process teams shows that the most effective teams draw on diverse skill sets and domains of expertise. Furthermore, as the government/contractor team irons out its different views and builds a common vision from sometimes very different goals, there are natural—but sometimes unsettling—negotiations that must take place. These can be openly vocal. Creating a context of candor is essential to the kinds of open discussion of joint and separate risks that are essential for Team Risk Management to work. This process of developing this context of candor requires courage, good will, and patience. It is very possible for a team to be "doing it right" but experiencing concerns about the team "taking so long to develop."

Or, in the terms of the July 1998 DoD guidance on integrated process/product teams,

> *...Because of the many, different traditionally competing functions involved in ...teams, team unity could prove a challenge...To facilitate consensus-building, team members must try not to be locked in by old paradigms. They should strive for innovation—to 'think outside the box'—and should not be afraid to voice concerns. Thus, an operating rule ... is 'don't shoot the messenger.' ... (A team) will at least to some degree be constantly subjected to ... traditional pressures ... and must be diligent in its efforts to overcome the hurdles. ... Once set up and operating, (the team) must remain focused on improving the team's effectiveness and taking every opportunity to make the changes that move the team closer to the ideal (team) environment."*

Members of the CCD Team Risk Review reached high performance as a team, as well as high technical performance results through application of joint Risk Management. This level of achievement is a tribute to the "stick-to-itiveness" of the respective TRR members, and most especially, to the model joint leadership of the government and contractor managers. The CCD division chief and his contractor managers formed a leadership team that was solid in its commitment to the process of Risk Management, and consistently exhibited their commitment as leaders to make it work.

5.3.2.1.5.5 Government/Contractor Partnerships in Other Divisions

As identified in the discussion for each division, the approaches to government/contractor Risk Management partnerships were defined differently by each division. While full-fledged monthly Team Risk Reviews occurred only in the CCD, Segment 2 and Segment 32 also created stronger Risk Management partnerships with their contractors.

With clear leadership by the Segment 2 division chief, this division strengthened its own Risk Management process, and then expanded that to its contractors. In fact, Segment 2 project managers provided knowledge transfer from their segment's Risk Management workshop and Risk Clinic to their contractors. Gradually, those contractors aligned their Risk Management processes with the Segment 2 process, and strengthened their Risk Management discipline to become more proactive in the identification and mitigation of risks.

Segment 32 actually engaged its contractors in a collaborative process of earlier definition of schedule delays and appropriate mitigations. The Segment 32 division chief retained vigilance and insight into the Risk Management efforts of contractors. Based on the growing maturity of Risk Management in Segment 32, the division chief moved forward an expanded discussion with contractors on risk analysis and mitigation strategies. The result was that the government/contractor relationship changed over a period of several months from one of parallel risk information and management, to a closer Risk Management partnership with greatly expanded shared information.

While Segment 5 continued with a primary focus on contractor Risk Management efforts, the division chief and other Segment 5 members collected and brought to the attention of the ESRT Segment 5 risks, involving monthly government/contractor discussions on the status of their risks from a government perspective.

5.3.2.1.6 Value of Risk Management for Segment 4

The value of Risk Management continues to be one of the primary criteria in Segment 4, and thoughtful consideration by many team members has provided a growing list of benefits for their program operations, including:

- Risk Management focuses random complaints into meaningful tasks with meaningful objectives.

- Risk Management provides data and specific plans to present to senior management, with reasoned proposals for action, persuasive requests for additional resources, definitions of readiness for further stages of a project, and guidelines for where initial operational capability (IOC) can likely be declared.
- Before Risk Management, contractors established the cost, schedule, and performance risks on a contract. After Risk Management installation, the division could clarify risks from the *government's* perspective.
- Government accountability was enhanced as was the quality of information available for executive oversight of missions, for national decision-makers and military customers. The effectiveness of acquisition programs was also supported. This was and is seen by Segment 4 as a primary benefit: government program management relies upon successful program delivery.
- Risk Management reduces a tendency to "blame the culture," improves the quality of data, and encourages candor in describing mission performance as objectively as possible.
- At the same time, Risk Management provides senior management with the ability to hold programs more accountable by identifying risks early and introducing mitigation plans soon enough to support downstream success.
- The Segment 4 division chief alerted staff members to stay focused on their performance, rather than that of others, and to be as candid and cooperative as possible in system interchanges.
- Divisional Risk Management provided the ability for Segment 4 to identify and usefully describe risks that Segment 4 could not mitigate on its own. These became system-level risks, and supported the system's ability to assess risks at that level.
- As a result of Risk Management, an improved EIS team environment developed.

5.3.2.1.7 Obstacles and Counter-Incentives to Risk Management

The following obstacles and counter-incentives can harm a Risk Management installation effort:

- Backstage negotiations can negatively impact Risk Management practices when special favors or exemptions are sought and granted.
- Some individuals in the system criticize the very practices that help improve programs.
- Initially, introduction of a Risk Management culture leads to increased accountability and openness, which challenges organizational members to change their behaviors. This is always an initial struggle.

5.3.2.1.8 Success Stories for Segment 4 Risk Management

Segment 4, as the pilot organization, had an opportunity to mature its Risk Management process significantly. As is the case with any improvement process, Risk Management repays discipline and diligence. As can be seen from the narrative, the CCD division encountered foreseeable challenges to changing the way it did business to incorporate Risk Management

practice. The division's focus on the value of Risk Management served as a touchstone throughout the effort to ensure that gains outweighed costs in Risk Management processes. As a result of a disciplined process and the length of time spent in working with Risk Management processes (including the interface and coordination with system-level and other divisional Risk Management processes), there were a number of "success stories" from Segment 4, which are presented in the following examples.

Example 1

Circa March 1998 the Segment 4 Command and Control Segment Program suffered a major setback when it failed to successfully meet its pre-ship review (PSR) milestone. The PSR was the control gate that signified that the segment had successfully completed its development efforts at the factory and was ready to make the transition to an integration, checkout, and test (IC&T) environment at the operational facility.

The development efforts leading up to the PSR had been tracked as one of first segment risks since August 1997 when the pilot Risk Management program was initiated. Mitigation plans had been put in place that included enhanced metrics collection and reporting as well as focus teams to concentrate on key technical drivers. In spite of the increased emphasis and attention placed on this effort and repeated warnings by the government team, the contractor's program manager neglected to adhere to or enforce the requisite programmatic rigor; the PSR failed.

The PSR failure resulted in a significant replan of the program and the development of a more detailed risk mitigation plan. Key aspects of the mitigation plan were the replacement of critical management personnel, the adoption of a more rigorous and insightful scheduling methodology, the conduct of CAIV (cost as an independent variable) trades to regain cost and schedule margin, the development of phased delivery schedules, incremental operability/functionality sell-off, and increased emphasis on early and informal interface testing.

Using the phased delivery methodology or Transition Element Sets (TES) as they became known, TES 1 was defined as the most critical as it provided the basis upon which all-subsequent TES would be built. This being the case, a risk was opened addressing the on-time delivery of TES 1 and a mitigation plan was developed.

The TES 1 mitigation plan was converted into a "waterfall chart," an adaptation of the mitigation plan plots discussed in SEI's *Continuous Risk Management Guidebook*, Appendix A, Chapter A-16, and provided the mechanism for monitoring and reporting progress against the plan. The mitigation plan identified key events that were to occur, and the associated timeframe that would buy down the risk's exposure. When the inevitable "surprises" occurred, the plan was updated to reflect the realities of what had occurred followed by an updated mitigation strategy. The development of the plan and a rigid adherence to the programmatic methodology that was formulated to manage the risk followed, and the risk was successfully closed when the segment delivered, ahead of schedule, and achieved its performance goals.

This risk also provided an opportunity for the management team to experiment with the merging of Risk Management and earned-value management techniques. This was facilitated by the contractor's ability to segregate the efforts associated with the component parts of the phased deliveries. The ability to collate data on the segregated financial, schedule, and technical components allowed the team to provide an integrated waterfall chart that mapped the risk mitigation activities against the budgeted baseline and the earned-value metrics (CPI, SPI, and TCP-LRE).

Example 2

The Segment 4 Command and Control Segment provides the infrastructure that manages the interfaces between the NRO's ground- and space-based resources. The segment is the latest in a series of C&C architectures and has the responsibility for managing not only the next generation of resources, but also the legacy components. As such, the segment is highly dependent on changes that are being flowed into the existing systems and for ensuring that current capabilities are not "deplenished" (i.e., the user will not see existing capabilities disappear that were not planned to disappear). In general a rigid configuration management (CM) process mitigates this "deplenishment" risk. Unfortunately, experience has shown that below a certain level of CM control, changes can be made to a "derived requirement" or an "implementation" that will not necessarily drive a higher-level RFC (request for change) that would be assessed for impact. But these lower CM-level changes could significantly affect end-user satisfaction if they are not incorporated into follow-on systems. This risk was much more difficult for the developers to mitigate because the drivers for this risk were deemed to be outside the span of control of the development segment. Therefore this risk was assigned to a "watch" category at the segment level, but some proactive steps were initiated to help support the mitigation of this risk. A key mitigation initiative was to more fully integrate the development team into the operational environment where team members would gain first-hand knowledge of most of the changes that had the potential to impact the follow-on developments. Although this effort did not capture all the lower level changes, nor changes that had been incorporated before the mitigation plan was instantiated, it did capture a majority of the potential impacts. Perhaps more importantly, the identification and quantification of the risk alerted senior management to the fact that changes that they were not privy to, because of the CM level of change, were being incorporated and presented as a significant risk to future users and complaints could ripple through the most senior levels of the NRO.

Example 3

The Segment 4 Command and Control Segment's performance is highly dependent on very sophisticated algorithms. In all instances the parameters that drive these algorithms are provided to Segment 4 by the interfacing segments. In some unique instances the interfacing segment also provides the models and equations. These data deliveries are typically provided by periodic database deliveries to Segment 4. As the interfacing segments mature through their development effort the definition and granularity of their knowledge of their design also

changes, which causes the data, models, and/or equations to further perturbate. These "as-built" changes also ripple into the C&C architecture in the form of data drive changes. As these changes occur later in the development cycles their impact can be many fold more significant to the receiving segment.

It was noted in previous programs that the attention to detail needed to assure that the database deliveries were adequate to support Segment 4 development and testing was not consistent across the numerous delivering segments. A number of risks were opened to address each of the delivering segments, but is discussed here as one generic risk.

Initially there was an attempt to manage this risk at the segment level because the resources required to ensure the quality of the delivered data resided with numerous other program managers. The segment put this risk on a "watch" list, but also took some proactive mitigation steps by working with the delivering segments to help audit and quality-check the data prior to delivery.

By putting together a cogent impact assessment and through repeated briefings to senior management this risk was eventually elevated to a system-level risk for joint mitigation by all parties.

As a result of this enhanced attention the quality of the data deliveries and their timeliness improved substantially.

Example 4

In 1997 the program embarked on a path to change the methodology by which it would 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 provided an easy avenue for the "deplenishments" noted in Example 2 to occur. To address the concern over diverging baselines, an Integrated Development and Maintenance Organization (IDMO) was developed. The IDMO would adsorb the maintenance functions traditionally managed by the operational site and integrate them into the development organization. The intent was to gain the synergy available through a single reduced staff that would manage a consolidated maintenance and development effort.

The advent of an IDMO was not readily embraced by the O&M organization, whose members believed that it took away some of their flexibility to utilize level-of-effort (LOE) resources to address the "good idea *du jour*" and required a scheduling discipline that was contrary to their existing business practices. In addition, their maintenance budget would be turned over to development.

It was the availability of budget that resulted in the identification of the first IDMO risk. The risk was that the original O&M program might not have budgeted for sufficient resources to support the new architecture that was being delivered. If the financial resources were inadequate then the probability of retaining critical skills and achieving the segment's required availability was problematic.

As the details of the risk were developed it turned out that there was indeed a significant budget shortfall. By providing this early identification the management team was able to provide a budget wedge and secure the funding needed to acquire the key resource and meet the availability requirements.

Example 5

Many of the functions of the Segment 4 Command and Control Segment are accomplished by the use of what is called engineering software (ES/W) code that supports specific engineering or analytical functions. Although any engineering code is suppose to be non-mission-critical in nature, over time the legacy operational systems have become dependent upon ES/W to conduct day-to-day operations and have elevated it to criticality.

One of the earliest risks identified by the segment was the potential that there was some ES/W in use that the current development effort was not going to re-deliver as CM controlled development code—or worse yet it would not be available as ES/W that the users of the follow-on systems would need based on their dependence of the same ES/W functionality in the legacy systems.

As with many of the risks identified by the segment, the resources and knowledge base that could mitigate this risk were managed external to the segment and through several separate contractual relationships.

The segment initially placed this risk on its "watch" list, but to help mitigate it worked very closely with the operational elements over an extensive period of time to identify shortfalls.

In spite of numerous audits, it was only through the persistence of the segment in keeping management's attention focused on this risk that the right resources were finally marshaled and a definitive closure plan developed.

5.3.2.1.9 Lessons Learned for Segment 4

See Chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

5.3.2.2 Segment 32 Risk Management

Segment 32, the second division to install Risk Management, is headed by Lt. Col. Mike Rhodes (the only Air Force officer who has been in divisional leadership throughout the two-year rollout and installation process, though Col. Steve Wojcicki was acting chief for Segment 5 for a few months in 1999).

Segment 32's management style was perhaps the most horizontal in the organization. Prior to the advent of Risk Management, this staff already met frequently as a team and members were skilled at open dialogue and joint problem-solving discussions. However, their skills for arriving at and maintaining consensus were still developing. Nevertheless, the experience of working as a team was not new to this division.

5.3.2.2.1 Initial Installation of Risk Management at Segment 32

Having understood from the IDP program director that Risk Management was to be incorporated into IDP's way of doing business, the Segment 32 division chief accepted this challenge with leadership statements of his own. He announced to his team that Segment 32 would move ahead to "be the best" at IDP in Risk Management. As a result, he scheduled Segment 32's IDP Risk Management Training course and Risk Clinic within two weeks of each other. Because each of these activities requires an investment of two entire days of division staff time—and ongoing scheduling challenges have made the division very selective about time investments—this decision sent a message to the division chief's team about the seriousness of his commitment.

The outcome of the Segment 32 Risk Clinic was a Risk Management plan, which defined the segment's initial Risk Management process. Following the Risk Clinic, the division further agreed to an offsite meeting in June 1998 to brainstorm, analyze, prioritize, and create mitigation plans for top risks. This offsite meeting—named a "risk roundup" by Segment 32 team members, both to indicate their intention to identify and compile all their risks for the first time, as well as to distinguish their team culture—was held three weeks after the Risk Clinic. Dedicating the entire team and its resources to an additional event, hard on the heels of the Risk Clinic, was further evidence of the importance of Risk Management to this division. Upon returning from the offsite, one of the staff members undertook creation of a risk database, which he constructed in Microsoft Access. This database was intended for ultimate presentation and consideration by the ESRT as a system-level tool, based on the original leadership decision in spring 1998 that "best practices" in each division would be encouraged and decided upon downstream.

5.3.2.2.2 Segment 32 Risk Management Process

Since the risk roundup, the division has not held regular risk meetings or a Team Risk Review with its contractors. However, according to the division chief, "Risk is now in people's awareness—staff routinely raise risk issues, identify new risks, track open risks on their risk

list, etc., at staff meetings, PMRs, even in hallway conversations." Indeed, the division chief named the most valuable asset of Risk Management as the "Risk Management mindset"—people thinking in terms of potential risks and what to do about them in advance.

The risk list is updated as mitigation plans succeed or change, and as old risks create new risks or issues, and as new risks emerge. Because a widely accepted test of culture change is whether the new concepts and behavior are "in the drinking water," integration of risk awareness and concern to this level would indicate that there has been a genuine evolution in thinking and acting on risk. The division chief and some of his staff are concerned about developing a Risk Management process that is streamlined and therefore enacted (rather than postponed). There are plans to review the division's process as well as its risk list at another offsite meeting.

5.3.2.2.3 Segment 32 Government/Contractor Risk Management Relationship

In addition to its risk database, the division also created a scheduling-forecasting tool. Segment 32 has no money to cover unexpected events at this point. There is no trade space possible for performance either, because all of this work has been completed. Therefore, the only arena where there is control is scheduling. Over the long term, Segment 32 had experienced a low level of confidence in the contractor's scheduling projections, which had repeatedly proven to be inaccurate (and were extended).

To address this issue, one of the Segment 32 staff members designed projection charts based on probabilistic forecasting. These charts analyzed all subsystems and incorporated data from the trend history of prior performance and the scheduling of risks and issues. The charts allow "what-if" scenarios to be run for comparison among possible alternative courses of action. From weighing these scenarios, Segment 32 leads can select best solutions and develop strategies to manage the risks involved. A key result of introduction of these charts into the government/contractor discussions was to clarify to the contractor the pervasive pattern of scheduling difficulties, which facilitated a new level of partnership between government and contractor to work toward solutions together. Since there is no management reserve to cover costs, and additional costs must be funded by the contractor, this literal "buy-in" on the part of the contractor is critical.

This joint generation of solutions continues, with an increase in advanced identification of bottlenecks by the contractor, which allows for improved risk mitigation. Segment 32's focus is more on this growing working partnership with its contractor than on "passing risks up the chain to the system level."

5.3.2.2.4 Key Risk Management Success Factors for Segment 32

The Segment 32 chief pointed to two main factors in installing Risk Management successfully:

- Open communication. Everyone contributes; all are encouraged to "say their piece" so that there is no constraint on surfacing controversial or apparently distant-in-time risks, and so that the team can get out in front of risks before they become issues.
- Solid leadership and a strong team. Team commitment does not have to be complete for Risk Management to work, but there must be significant commitment and involvement. The role of the leader/sponsor is to steer the process and continue to reinforce its priority.

5.3.2.2.5 Benefits/Success Stories for Segment 32 Risk Management

When asked, "Honestly, has Risk Management made a difference in the way you do business?" the division chief reinforced the importance of the "risk mindset" and then identified three specific success stories:

- There was a system risk from the interface of Segments 5 and 32 and the ground station to produce high-quality images. Discussions of this risk eventually resulted in an interface test that will mitigate the risk and improve the ability to produce good imagery at IOC.
- Segment 32 has had success with the contractor in recognizing earlier that it could not meet payload because of bottlenecks and acknowledging that an "impossible schedule needed to be worked" resulting in more realistic scheduling.
- The contractor relationship has become a more open, collaborative partnership, though now it is "tougher because we are pushing them," but "we are now having more frank discussions."

5.3.2.2.6 Improvements Recommended by Segment 32 for System Risk Management

The ESRT "moves too slowly" and "focuses too narrowly" for successful system-level impact, according to this division chief. Programs are "moving faster than the ESRT 'do loop,' " and some form of effective interim mechanisms should be developed. Divisions are working interfaces that have risk aspects throughout the month.

At the same time, an important role for the ESRT is being neglected—that is, to "look downstream, at least one to two years ahead, to focus strategically (versus operationally) on potential system-level risks with new programmatic impact.

Finally (and this is also a lesson learned), for further NRO rollouts the Executive System-Level Risk Management Team leadership needs to be clear from the beginning about its policies for divisional development of Risk Management processes, tools, and formats. This is most apparent in regard to the Risk Management tool. For the RMT to be fully effective, the tool must be available on everybody's desktop.

In fact, particularly since Risk Management does take some additional time—though in the long run, there is ample evidence that overall time costs are reduced through reductions in

rework, fewer "pop-ups" in program issues, and other benefits—it would be wise to standardize some Risk Management practices right from the start. Rather than create an expectation that each division's "best practice" would be considered, compiled, and integrated, or that one practice would be selected for system-wide rollout—unless that approach is actually feasible—it would be more effective to simply select a joint approach and invite divisional participation so that staff members could improve it together.

5.3.2.2.7 The Segment 32 Definition of the "Ultimate Success" of Risk Management

The Segment 32 division chief described what, for him, is the ultimate test of system Risk Management: successful delivery of the entire program.

While Risk Management cannot guarantee success, this perspective suggests that effective assessment of the Risk Management program needs to be performed when the program is completed. Relative contributions and lessons learned can be appropriately weighed in the context of the overall program's outcome.

This comment reflects the perspective of a representative of the Acquisition Center of Excellence who said, "The real goal of Risk Management is delivery of successful programs."

5.3.2.2.8 Lessons Learned for Segment 32

See Chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

5.3.2.3 Segment 2 Risk Management

At the request of the Segment 2 division chief, information for this report on the specifics of the Segment 2 experience with Risk Management installation was provided by a senior technical project manager from the division, Tanya Wilkerson, and was confirmed by the division chief, Paul Albright. This project manager's perspective was especially helpful in that she is one of two staff members who have coordinated and supported ongoing Segment 2 Risk Management activities.

Engaging with Risk Management was a challenge for Segment 2, as this division was, as staff members would admit, initially skeptical. One reason for this was that Segment 2 was already practicing its own version of a government Risk Management process and needed to see value-added from the SEI approach before it would become fully engaged.

Nevertheless, Segment 2 did commit to undertake *both* the IDP Risk Management Course, as well as the Risk Clinic, which were scheduled approximately a month apart. All Segment 2 staff attended at least one of these sessions.

5.3.2.3.1 Risk Management Training and Clinic in Segment 2

During the Risk Clinic, Segment 2 members raised the issue of their existing Risk Management process, and sought to clarify what new tasks were being asked of them. In addition, the division chief discussed his lack of awareness that Risk Management had become a system-level mandate, directed by Program Director Al Krum. To address the need for these clarifications, the IDP program director visited the Segment 2 Risk Clinic to confirm that Risk Management was a system-level priority, and to respond to questions from the division staff.

Subsequently, a Segment 2 member captured the decisions from the Segment 2 Risk Clinic into the Segment 2 Risk Management plan, which has been modified over time to reflect actual practice variations.

5.3.2.3.2 Current Segment 2 Risk Management Process

From the start, as with Segment 32, Segment 2 chose not to have a separate Team Risk Review; rather, it chose to use its staff meetings for government Risk Management and the PMR for contractor Risk Management.

The current Risk Management process includes regular activities centered on weekly staff meetings. The process is as follows:

1. The project manager and another technical person capture Risk Management data from the staff meeting and enter it on the Segment 2 Risk Management spreadsheet.
2. The division chief then "racks and stacks" the risks, providing updates that have been collected from staff members individually.
3. Between meetings, staff members talk directly with the division chief and immediately send to the chief and the project manager email on new and current risks, along with other project information.
4. Finally, the project manager and her colleagues visit staff members to discuss current risk changes and new information related to specific risks, review mitigation plan "gates," and discuss other relevant factors.

Pending the full system-wide installation of the Risk Management tool, Segment 2 used primarily a "paper-and-pencil process," supplemented by direct discussion with the technical owners of specific risk areas, and supported by the spreadsheet.

The Segment 2 weekly staff meetings lasted one hour. "Because people receive the risk spreadsheet by email, all staff are informed before arriving at the staff meeting on the overall divisional risk picture," according to the Segment 2 project manager. The result is that "any person in the division can describe what is going on in the whole division."

Clearly, the Segment 2 Risk Management process is strongly leader-directed. Nevertheless, staff involvement has increased since the installation and rollout of Risk Management across IDP. Additionally, there is much more widespread staff awareness of overall divisional risks

and members are better able to consider interfaces among projects, as well as divisional interfaces across the system level.

The Segment 2 project manager confirmed that there is "ample room for disagreement;" if a staff person disagrees with the priority ranking or mitigation plan the Segment 2 chief has laid out, negotiation takes place.

Also, the Segment 2 team is reaching higher levels of discernment with regard to risks and issues: "pop-up risks are now spotted in the middle of handling an issue," and when a risk is spotted, the risk is taken seriously and acted upon. In turn, issues are sometimes worked as part of risk mitigation planning. These two activities, taken together, show that Segment 2 has a grasp of the essential complex interconnection between Risk Management and project/program management: risks can give rise to risks; risks can give rise to issues; issues can give rise to risks.

5.3.2.3.3 Comparison between Segment 2 Risk Management Process Before and After Risk Clinic

In response to a request for comparison of changes brought about in Segment 2 operations by the installation of an integrated approach to Risk Management, the project manager identified a number of areas where differences can clearly be observed:

Table 5: Differences Before and After Risk Clinic

BEFORE RISK CLINIC	AFTER
Risks were informally and only verbally discussed.	Risks are formally documented—the biggest change.
Staff members were usually familiar primarily with risks related to their own project or area.	A spreadsheet is available for all staff to review and is emailed to everyone periodically for review (at irregular intervals).
The division chief did virtually all risk analysis. The staff team identified risks at staff meetings. The division chief collected, decided go/no-go on specific risks, determined severity, and assigned mitigation actions.	Two project managers sit down with staff members to review risks, find out where risk mitigations are, what "gates" have been passed, etc.; shared information has created broader participation.
The contractor had identified risks, reporting on what had been done/planned but not in disciplined way.	The contractor provides waterfall charts at PMR (the waterfall chart is generated by the contractor) and reports every two months; charts are updated monthly.

There was continued use of contractor waterfall charts for some time after installation of divisional Risk Management.	The Risk Management tool is expected to generate waterfall charts with data input (the RMT did not originally generate government waterfall charts but had data available); government information is presented at the ESRT and other appropriate forums.
Risk identification was primarily by email or in direct discussions with the division chief.	Risks are now identified in a number of ways: directly in person to the director; with project managers in their regular rounds; or presented at staff meetings (after the chief has been informed).

5.3.2.3.4 Segment 2 Government/Contractor Risk Management Relationship

As with Segment 32, the Segment 2 government/contractor Risk Management working relationship is continuing to evolve.

In fact, one of the Segment 2 project officers recently took the initiative to work directly with the contractors to coach them on the knowledge base and process of Risk Management as practiced at IDP—what Segment 2 members are learning in the Risk Management training course and the Risk Clinic. This project officer has identified critical path areas where more disciplined Risk Management processes are encouraged for the contractor by Segment 2 government staff. As a result, the Segment 2 contractors are much quicker at recognizing and openly discussing when a schedule is unrealistic.

An issue in the discussions with the contractors was performance measures: earned value was not originally on Segment 2's contract, and was implemented at IDP after contract startup. The contractor has supplied a performance measures report, which includes schedule and cost drivers on risks and costs of impact. In addition to analysis of scheduling risks, Segment 2 is working with its contractor on additional pertinent risk metrics.

5.3.2.3.5 Benefits of Risk Management for Segment 2

The Segment 2 project manager identified four main benefits from Risk Management:

1. The division now formally documents its risks using its Risk Management spreadsheet to "rack and stack." Previously, risk discussions were not written down.

2. The contractor has become more involved and is using systemwide templates and processes; the contractor is supplying more—and more timely and pertinent—information than before.
3. The entire staff is more aware of the full list of Segment 2 risks, and is therefore more able to discuss interfaces among projects and offer good ideas to one another. Previously, risk discussions tended to occur in small groups only or between a risk process owner and the Segment 2 chief only; now there are fully engaged discussions on divisional risks across projects.
4. Segment 2 members realized that the Risk Management process is tailorable and evolutionary, not revolutionary. The gains are subtle but accumulate over time.

5.3.2.3.6 Improvements in Risk Management Recommended by Segment 2

Segment 2 members recommend the following improvements for the Risk Management process:

- Start risk identification by integrating it at the end of the Risk Clinic; it "would have jump-started the process a lot faster" and it would have been easier to schedule the time all at once.
- If better and clearer information about what to expect from what risk learning activity had been available it would have better set expectations for the Segment 2 team.
- It would be helpful to hold advanced discussions regarding trades, criteria for mitigation plans, and levels of risk tolerance a few weeks after the Risk Clinic.

5.3.2.3.7 Lessons Learned for Segment 2

See Chapter 6, "Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations."

5.3.2.4 Segment 5 Risk Management

Segment 5 was the fourth major division to undertake the IDP Risk Management training course. Virtually all members of Segment 5 participated actively and contributed to discussions during the session. Several members of the Segment 5 staff indicated an interest in (1) conducting their own Risk Clinic and (2) establishing a government Risk Management process.

However, Segment 5 said its contractor had for a long time operated its own Risk Management process. Eventually, the division chief of Segment 5, who initially was Chip Gilbert, provided an opportunity for his staff to choose whether to conduct a Risk Clinic or to at least engage in a risk identification/mitigation strategy-planning session. Again, several staff members were strongly interested in active engagement with Risk Management (and their interest continued over several months), but apparently they were overruled by those who were confident that the status quo was sufficient.

As a result, the contractors continued as the sole Risk Management practitioners in Segment 5. They regularly presented their identified risks, analysis, mitigation plans, and status to the government team members.

Meanwhile, there was encouragement from the program director to the Segment 5 division chief to "take back" some of the accountability for government Risk Management and program delivery insight, particularly after the Segment 5 contractor caused a major schedule slip. This event required the program director to apply for additional funds and time to remedy the slip, and led him to announce to all his division chiefs that he "wanted everyone to put their cards on the table," that he "only wanted to go once for resourcing support," and that he really needed "full information now."

However, still having not engaged in its own government Risk Management process, less than a year later Segment 5 encountered yet another major schedule slip.

Since that time, division leadership has changed. Segment 5 joined Segments 3 and 4 under the newly reorganized IDS program.

It is important to note the importance of avoiding over-hasty conclusions about the performance factors of Segment 5. In any organization, there are multiple co-factors that impact on organizational results. Just as government Risk Management cannot guarantee program success, neither can the absence of a government-directed process be held totally accountable for technical performance or scheduling gaps. And indeed, the long-term division chief regularly attended and participated in the ESRT and its system-wide Risk Management efforts.

Still, it is worth noting that Segment 5 was the only technical division that did not fully install a government-directed Risk Management system, relying solely on its contractors to safeguard its risks.

5.3.2.5 Segment 1 Risk Management

The Development Systems Division (the systems integrator)—Segment 1—also underwent an IDP Risk Management training session, though many of its members had attended those in other divisions. Still, because it was the division responsible for fostering and continuing the process and evolution of system-level Risk Management, staff members and contractors in this division believed that having the full training session would enable them to "be more responsible and capable in their role" on behalf of the entire system, according to the Segment 1 chief, Rob Moore.

However, since it is not strictly speaking a technical division, there was no expectation that Segment 1 would conduct a Risk Clinic. Yet, after the training session, Segment 1 became even more invested in mastering Risk Management, and considered conducting a Risk Clinic after all. Though this never came to pass, it is worth noting that there was lively interest in this division in assessing its own operational risks.

Given its pivotal role in system management, Segment 1 has been actively involved in the ESRT and its related activities. This division became owners of the tailoring and redesign of the Risk Management tool for system-level application. Also, the division coordinated a team of project managers, one or two from each division, who were known as the risk cadre and who were originally slated to serve as divisional trainers in Risk Management. For a short time, the cadre evolved to consider the impact of system-level approaches to Risk Management. Eventually, they provided valuable input to development of the Risk Management tool for system-level use, ensuring that the tool would be usable by each division.

At this time, Segment 1 has been subsumed by the reorganization, which has generated a systems-engineering organization under the leadership of former Program Director Al Krum. As a result, the division itself is no longer a player in system Risk Management. However, members of the former Segment 1 staff continue to play an active role in completing the system-level development and installation of the system Risk Management tool and in supporting Risk Management in various system-level meetings and forums.

6 Knowledge Management: Success Stories, Lessons Learned, and Next Steps/Recommendations

As evidenced by testimony of IMINT practitioners who mastered and incorporated Risk Management into the way they did business, Risk Management is more than an adjunct to program management. The emphasis in Risk Management on future-looking, proactive management of probable, high-impact, downstream events requires integration of smart thinking from across the organization. The "Risk Management awareness" described by the division director in Segment 32 helps programs use critical information to address all their issues more effectively.

The Segment 4 Team Risk Review has used the term "knowledge management" to convey this phenomenon. According to one core definition, knowledge management is

> *"the systematic process of finding, selecting, organizing, distilling and presenting information in a way that improves ... comprehension in a specific area of interest. Knowledge management helps an organization to gain insight and understanding from its own experience. Specific knowledge management activities help focus the organization on acquiring, storing, and utilizing knowledge for such things as problem solving, dynamic learning, strategic planning, and decision making. It also protects intellectual assets from decay, adds to firm intelligence, and provides increased flexibility."* <URL: http://www.bus.utexas.edu/kman>

As organizations become more acquisition-focused and must share knowledge across programs, businesses and the government are exploring knowledge management to discover opportunities for better programs. For example, the Air Force Office of Scientific Research, the Alfred P. Sloan Foundation, Xerox Corporation, and other companies sponsor the Knowledge Creation and Transfer, UC Berkeley Forum on Knowledge and the Firm.

Risk Management is really a process of developing a system-wide strategic process of knowledge management, as well as a methodology to surface and address technical and operational risks.

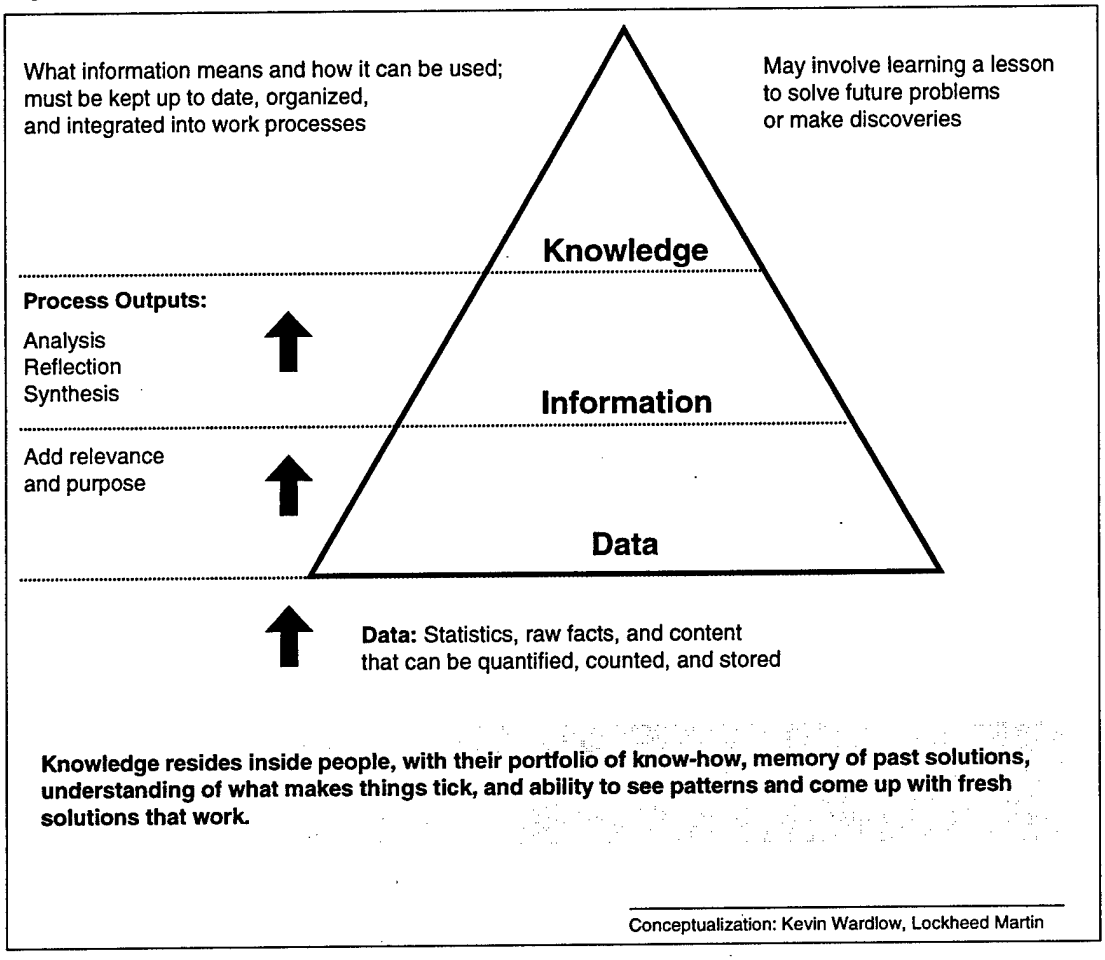
Observing the robust discussions on both program issues and program risks that occurred at the regular Team Risk Reviews, a contractor with Segment 4, Kevin Wardlow, designed a

schematic chart to define the differences between knowledge management and what could be identified as simply "data management" or "compilation of information." As indicated on this chart, "Knowledge resides inside people, with their portfolio of know-how, memory of past solutions, understanding of what makes things tick, and ability to see patterns and come up with fresh solutions that work."

The "knowledge management pyramid" entails transformation of data into useful information, and information to knowledge that can be applied to address problems or generate innovation.

The schematic below outlines the pyramid of knowledge management:

Figure 10: Pyramid of Knowledge Management



The knowledge pyramid is progressive, building from data to information to knowledge that can be managed:

1. *Data* comprises statistics, raw facts, and other content that can be quantified, counted, and stored. It is transformed into information through the addition of relevance and

purpose. In Risk Management, the TRR provides a forum where the combined expertise, technical focus, organizational level, and backgrounds of participants can compile a meaningful body of data.

Example of data: Operating system upgrades are hard. There have been past histories of upgrade problems. There have been several changes in staff with critical skills in the last year. Government milestone targets have shifted to the left.

2. *Information* is produced through analysis, reflection, and synthesis of data. In the TRR process, a member brings forward potential risks, and other TRR participants then add insights and critical relevant information on whether or not a given issue is, in fact, a risk that bears further analysis and addition to the risk list. If there is agreement on risks from participants in the TRR, and the division chief signs off on them, the risks are then formulated into risk statements, with clear context that will have meaning broadly across the organization. Risk information is logged onto the risk information sheet, and risks are analyzed, prioritized, and combined where appropriate. In other words, data becomes information that can be leveraged for further understanding and action on risks.

   Example of information: We have an operating system upgrade to be done. We know that the vendor will maintain our system but versions change. Soon the vendor will stop supporting this version; therefore we know we will have to do an upgrade. Also, there will need to be code changes on the operating system, which will compound the issue. With the schedule shift to the left, there may not be adequate time to allow for full performance testing. This in turn could cause trouble in critical interfaces, as well as incursions into the critical path.

3. *Knowledge* is derived by organizing and conceptualizing information so that it is useful. Alternative scenarios may be configured, creative solutions found, and relevant actions taken. Knowledge is managed when a team is able to forge its combined expertise, repository of past solutions that might, with modifications, apply to the new situation, understanding of root causes, and analysis of patterns. The TRR achieves knowledge management through integration of the multiple perspectives represented on the TRR; managers and members come to value contradictory information and perspectives as contributions to stronger solutions. The TRR begins to formulate a clear idea of what the risks are and what needs to be done about them. These parameters will need to be informed by the composite knowledge of TRR members into "knowledge management" by the integrated team.

   Example of knowledge: An assessment is made of the size of the upgrade and its resulting potential impact. Analysis of past history with similar upgrades in tight timeframes yields a number of subtle as well as major impacts. Experience with upgrades provides some possible alternative scenarios to optimize schedule lulls in parallel maintenance activities that might free up some skilled people who could be cross-utilized. Management provides understanding of possible trades on scheduling priorities. Experienced staff can speculate based on work processes about such possibilities as maintaining a separate baseline, working in parallel, merging systems later, and running regression tests to verify that no adverse effects occur. By pooling knowledge in such discussions, decisions can be made about how to build plans with optimum actions, quantifiable measures, and milestones to execute the plans.

Knowledge management takes a strategic focus to determine what kinds of data should be collected and to arrive at information targeted to the organization's business goals, which in turn will create a context in which knowledge becomes a value to the organization. Risk Management, when fully performed, yields this level of knowledge management.

Indeed, Risk Management compiles, analyzes, and prioritizes risk data, transforms this data into risk information that can support planning and decision-making, and then leverages that information into an assessment of program and system integration of efforts and re-planning at a higher level of system insight than was possible before.

Critical to this knowledge management process is learning from mistakes and understanding how approaches could be improved; learning does not only come from successes. A cautionary note: true knowledge management derives from converged agreements on just what lessons were learned, and how important they were. Without a formal process, such as that practiced by the U.S. Army's After Action Review, the lessons themselves must be viewed at the level of "information" rather than "knowledge." Hence, the lessons and success stories in this section remain tailored to the originating divisions or units from which they were derived. In the future, IMINT may wish to undertake a formal, disciplined process to synthesize and extract key knowledge outcomes into a system repository.

The sections below contain lessons learned, together with next steps and recommendations, as well as success stories for each IDP division that practiced active Risk Management—Segment 4, Segment 32, and Segment 2.

6.1 Success Stories for the IDP Program

As can be seen from the experiences across the IDP program, Risk Management provided, in a relatively short time, some rich successes. Many of these were critical to program delivery and achieved gains—on budget, schedule, technical performance, and the organization—that were significant. Following are those success stories with considerable positive impact on overall program success.

Example 1

Circa March 1998 the Segment 4 Command and Control Segment Program suffered a major setback when it failed to successfully meet its pre-ship review (PSR) milestone. The PSR was the control gate that signified that the segment had successfully completed its development efforts at the factory and was ready to make the transition to an integration, checkout, and test (IC&T) environment at the operational facility.

The development efforts leading up to the PSR had been tracked as one of first segment risks since August 1997 when the pilot Risk Management program was initiated. Mitigation plans had been put in place that included enhanced metrics collection and reporting as well as focus teams to concentrate on key technical drivers. In spite of the increased emphasis and attention

placed on this effort and repeated warnings by the government team, the contractor's program manager neglected to adhere to or enforce the requisite programmatic rigor; the PSR failed.

The PSR failure resulted in a significant replan of the program and the development of a more detailed risk mitigation plan. Key aspects of the mitigation plan were the replacement of critical management personnel, the adoption of a more rigorous and insightful scheduling methodology, the conduct of CAIV (cost as an independent variable) trades to regain cost and schedule margin, the development of phased delivery schedules, incremental operability/functionality sell-off, and increased emphasis on early and informal interface testing.

Using the phased delivery methodology or Transition Element Sets (TES) as they became known, TES 1 was defined as the most critical as it provided the basis upon which all-subsequent TES would be built. This being the case, a risk was opened addressing the on-time delivery of TES 1 and a mitigation plan was developed.

The TES 1 mitigation plan was converted into a "waterfall chart," an adaptation of the mitigation plan plots discussed in SEI's *Continuous Risk Management Guidebook*, Appendix A, Chapter A-16, and provided the mechanism for monitoring and reporting progress against the plan. The mitigation plan identified key events that were to occur, and the associated timeframe that would buy down the risk's exposure. When the inevitable "surprises" occurred, the plan was updated to reflect the realities of what had occurred followed by an updated mitigation strategy. The development of the plan and a rigid adherence to the programmatic methodology that was formulated to manage the risk followed, and the risk was successfully closed when the segment delivered, ahead of schedule, and achieved its performance goals.

This risk also provided an opportunity for the management team to experiment with the merging of Risk Management and earned-value management techniques. This was facilitated by the contractor's ability to segregate the efforts associated with the component parts of the phased deliveries. The ability to collate data on the segregated financial, schedule, and technical components allowed the team to provide an integrated waterfall chart that mapped the risk mitigation activities against the budgeted baseline and the earned-value metrics (CPI, SPI, and TCP-LRE).

Example 2

The Segment 4 Command and Control Segment provides the infrastructure that manages the interfaces between the NRO's ground- and space-based resources. The segment is the latest in a series of C&C architectures and has the responsibility for managing not only the next generation of resources, but also the legacy components. As such, the segment is highly dependent on changes that are being flowed into the existing systems and for ensuring that current capabilities are not "deplenished" (i.e., the user will not see existing capabilities disappear that were not planned to disappear). In general a rigid configuration management (CM) process mitigates this "deplenishment" risk. Unfortunately, experience has shown that below

a certain level of CM control, changes can be made to a "derived requirement" or an "implementation" that will not necessarily drive a higher-level RFC (request for change) that would be assessed for impact. But these lower CM-level changes could significantly affect end-user satisfaction if they are not incorporated into follow-on systems. This risk was much more difficult for the developers to mitigate because the drivers for this risk were deemed to be outside the span of control of the development segment. Therefore this risk was assigned to a "watch" category at the segment level, but some proactive steps were initiated to help support the mitigation of this risk. A key mitigation initiative was to more fully integrate the development team into the operational environment where team members would gain first-hand knowledge of most of the changes that had the potential to impact the follow-on developments. Although this effort did not capture all the lower level changes, nor changes that had been incorporated before the mitigation plan was instantiated, it did capture a majority of the potential impacts. Perhaps more importantly, the identification and quantification of the risk alerted senior management to the fact that changes that they were not privy to, because of the CM level of change, were being incorporated and presented as a significant risk to future users and complaints could ripple through the most senior levels of the NRO.

Example 3

The Segment 4 Command and Control Segment's performance is highly dependent on very sophisticated algorithms whose basis is formed by a series of models and equations that capture the unique aspects of the space-based platforms and the ground-support infrastructure. In all instances the parameters that drive these algorithms are provided to the Segment 4 by the interfacing segments. In some unique instances the interfacing segment also provides the models and equations. These data deliveries are typically provided by periodic database deliveries to Segment 4. As the interfacing segments mature through their development effort the definition and granularity of their knowledge of their design also changes, which causes the data, models, and/or equations to further perturbate. These "as-built" changes also ripple into the C&C architecture in the form of data drive changes. As these changes occur later in the development cycles their impact can be many fold more significant to the receiving segment.

It was noted in previous programs that the attention to detail needed to assure that the database deliveries were adequate to support Segment 4 development and testing was not consistent across the numerous delivering segments. A number of risks were opened to address each of the delivering segments, but is discussed here as one generic risk.

Initially there was an attempt to manage this risk at the segment level because the resources required to ensure the quality of the delivered data resided with numerous other program managers. The segment put this risk on a "watch" list, but also took some proactive mitigation steps by working with the delivering segments to help audit and quality-check the data prior to delivery.

By putting together a cogent impact assessment and through repeated briefings to senior management this risk was eventually elevated to a system-level risk for joint mitigation by all parties.

As a result of this enhanced attention the quality of the data deliveries and their timeliness improved substantially.

Example 4

In 1997 the program embarked on a path to change the methodology by which it would 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 provided an easy avenue for the "deplenishments" noted in Example 2 to occur. To address the concern over diverging baselines, an Integrated Development and Maintenance Organization (IDMO) was developed. The IDMO would adsorb the maintenance functions traditionally managed by the operational site and integrate them into the development organization. The intent was to gain the synergy available through a single reduced staff that would manage a consolidated maintenance and development effort.

The advent of an IDMO was not readily embraced by the O&M organization, whose members believed that it took away some of their flexibility to utilize level-of-effort (LOE) resources to address the "good idea *du jour*" and required a scheduling discipline that was contrary to their existing business practices. In addition, their maintenance budget would be turned over to development.

It was the availability of budget that resulted in the identification of the first IDMO risk. The risk was that the original O&M program might not have budgeted for sufficient resources to support the new architecture that was being delivered. If the financial resources were inadequate then the probability of retaining critical skills and achieving the segment's required availability was problematic.

As the details of the risk were developed it turned out that there was indeed a significant budget shortfall. By providing this early identification the management team was able to provide a budget wedge and secure the funding needed to acquire the key resource and meet the availability requirements.

Example 5

Many of the functions of the Segment 4 Command and Control Segment are accomplished by the use of what is called engineering software (ES/W) code that supports specific engineering

or analytical functions. Although any engineering code is suppose to be non-mission-critical in nature, over time the legacy operational systems have become dependent upon ES/W to conduct day-to-day operations and have elevated it to criticality.

One of the earliest risks identified by the segment was the potential that there was some ES/W in use that the current development effort was not going to re-deliver as CM controlled development code—or worse yet it would not be available as ES/W that the users of the follow-on systems would need based on their dependence of the same ES/W functionality in the legacy systems.

As with many of the risks identified by the segment, the resources and knowledge base that could mitigate this risk were managed external to the segment and through several separate contractual relationships.

The segment initially placed this risk on its "watch" list, but to help mitigate it worked very closely with the operational elements over an extensive period of time to identify shortfalls.

In spite of numerous audits, it was only through the persistence of the segment in keeping management's attention focused on this risk that the right resources were finally marshaled and a definitive closure plan developed.

Further Examples

When asked, "Honestly, has Risk Management made a difference in the way you do business?" the division chief reinforced the importance of the "risk mindset" and then identified three specific success stories:

- There was a system risk from the interface of Segments 5 and 32 and the ground station to produce high-quality images. Discussions of this risk eventually resulted in an interface test that will mitigate the risk and improve the ability to produce good imagery at IOC.
- Segment 32 has had success with the contractor in recognizing earlier that it could not meet payload because of bottlenecks and acknowledging that an "impossible schedule needed to be worked" resulting in more realistic scheduling.
- The contractor relationship became a more open, collaborative partnership, though now it is "tougher because we are pushing them," but "we are now having more frank discussions."

6.2 Government/Contractor Success Stories

The contractor organizations pay close attention to rapid response to crises, while maintaining a long view to capture lessons into a "virtual organization" library. The organization communicates its knowledge assets via a Web page that provides continuous improvement as well as current project/task information. As each project is brought to closure, there is in the

project plan a trigger to conduct "lessons learned" reviews. When the project team's proposed lessons are compiled, they are sent to a review board and are adjudicated as to whether they are durable lessons to include in the knowledge assets repository.

When necessary, this process can be managed very quickly for project lessons with broad system implications: a recent correction was completed in 24 hours, and the "lessons learned" package was sent out immediately to help reduce recurrences in other projects. This process leverages Risk Management through an almost instantaneous transmission of information about critical project improvements.

The contractor Risk Management process also acknowledges that human error is inevitable. "There may be nothing wrong with the plan, the project, the technical design, et cetera," said one contractor manager, "we still have to be alert to the inevitable human errors. We 'harden the system' to human error by integrating performance monitors and verifications at regular checkpoints."

Within this context of risk alertness, there have been a number of success stories that the contractors see as attributable to the strengthened government/contractor partnership, including the following:

1. Hitting the SCR-TE 1 schedule date. Risk Management provided simplification for development, which assured that the program reached the target date (against widespread expectations that it would not be made).
2. Improving CCD critical skills. The combined forces and best thinking of government and contractor were marshaled to resolve the issue of Segment 3 critical skills. The follow-on contractors built a diagram that showed the *quantified* impact of the loss of critical skills on system availability over time, which calculated the mean time between failure breaks, figured in lag times as well as specific system parts that could break, and their further impact.
3. The follow-on program was responsible for converting mainframe-hosted engineering software to the distributed system. Given schedule constraints and associated risks, the contractor redesigned the system architecture platform so that tools could not only function in the new environment, but some software could be left on the mainframe to save time and effort in rewriting and conversion, and focus on the interfaces created.

   To accomplish this, the contractors defined the risks involved, examined alternative mitigation strategies, including thinking through what would happen if they stopped the conversion process and worked the interface at given points in the development. To build a solution, they designed prototype plans to prove concept, measured observables to gauge success potential, analyzed the schedule against the critical path, and identified a "point-of-no-return" contingency trigger date. All risk planning was completed in a week and a half. As a result, 20 of 30 applications were saved, in addition to more than 50% of the originally planned effort.

   The successes here were multiple: improved schedule, reuse, time, and skills released for other pressing needs.

4. Delivery #1 Transition: the contractor risk mitigation was the entire transition plan. To accomplish the transition, they began by asking key questions, such as: Provided Delivery #1 was transitioned successfully, what would happen if the contractor was not ready? What would "ready" look like?

   To mitigate this portfolio of risks, the contractors reviewed a robust view of the risk taxonomy, including technical review, program management, and maintenance. Over a two-month period, they wrote a 100-page plan with 47 identifiable tasks, individual assignments, and due dates which were statused weekly. As a result, when transition occurred, technical readiness was in place. With no perturbations, the change of ownership was seamless and invisible to anyone outside the process.

6.3 Lessons Learned, Next Steps/Recommendations

This "lessons learned" section identifies areas for further exploration, and provides initial indicators as to potential improvements, rather than an authoritative list of lessons that should be acted upon immediately. Even prior to formal system consensus on the right lessons, differing perspectives from the divisions shed light on the various Risk Management process installations.

6.3.1 Segment 4 Lessons Learned, Next Steps/Recommendations

6.3.1.1 Segment 4 Lessons Learned

Segment 4 has identified, over the course of its two-year effort, lessons learned, next steps, and recommendations for improvement. Taking responsibility to not only practice Risk Management but to share growing knowledge and suggestions is very much part of constructive communications for Risk Management. The lessons drawn from Segment 4's Risk Management process are founded in the segment's growing realization that Risk Management succeeds best where ideas and input are widely encouraged, and then debated openly to forge the best solutions.

The lessons to date that Segment 4 endorses are the following:

- Real process improvement, as well as systemic and structural change are requirements for Risk Management success. Those who introduce Risk Management—whether it is the SEI or the government—have a responsiblity to stimulate the organization to question its standard operating procedures.
- Meetings in which "everyone's cards are placed on the table"—such as the one between Segment 4 and the SEI—need to happen, early in the process, and with every key decision maker and division.
- In change management, which is what Risk Management is, the sponsor needs to be the biggest ally. The senior executive in the system must routinely reinforce Risk Management thinking, asking about the Risk Management history of "pop-up" issues that appear.

- The rollout and installation approach needs to do a better job of explaining how Risk Management will "help me get my job done every day."
- Initial organization preparation for a Software Risk Evaluation should include
  - a glossary of commonly used terms
  - alignment of the description of Risk Management with the organization's own terminology and language. (One division member commented, "We are not interested in learning a new vocabulary—that's not value-added.")
- Clearer definition should be done to explain the difference between the Risk Management model approach, and how the model can be leveraged to real-world programs: the "process provides a bridge between the academic and applied engineering," according to Tommy Meeker, then a Segment 4 area manager.
- The CCD program director created a draft CCD Risk Management flowchart overnight during the Risk Clinic, and received CCD team approval. Here, one valuable lesson learned is that the creativity of the leader and the team should be encouraged to assure buy-in to the Risk Management process.
- At the clinic, the team built a "flight plan" for Risk Management that team members were confident would work, and which they knew they could modify. "This was a very important facet of Risk Management for this team. From that day forward, we believed that 'if we plan the plan, we can fly the plan,'" a team member said.

6.3.1.2 Segment 4 Next Steps/Recommendations

Recommendations from each division are the repository of assets that can be leveraged for future Risk Management efforts not only in EIS but across IMINT and elsewhere at NRO. Recommendations from Segment 4 include the following:

- *For system-level Risk Management, categorize a relativity scale for risk attributes.* That way, while attribute criteria from each division may be tailored to that specific division's risks (together with very different parameters of funding levels, schedule, and technical performance), there can be understanding *across* divisions as to relative impact and importance. Still, while this recommendation is intended to support system-level decision-making across divisions, "there will continue to be a need for critical thinking—no cross-organizational comparison will yield easy answers," according to a team member.
- *Culture management is necessary in Risk Management.* "People have to internalize Risk Management for it to be successful, and this takes awhile for a system to accomplish. Risk Management is not a 'quick fix.'"
- *Reasonable expectations must be set for what Risk Management can accomplish.* While it can improve—and sometimes greatly improve—the likelihood of program success, "Risk Management is not a 'silver bullet' either—it cannot provide a crystal ball and eliminate all risks or issues." What Risk Management *can* do, if successfully practiced, is increase positive results and reduce the severity and occurrence of problems.

6.3.2 Segment 32 Lessons Learned, Next Steps/Recommendations

6.3.2.1 Segment 32 Lessons Learned

Lessons drawn from the experiences in Segment 32 were based on that segment's particular needs, and included the following:

- Effective Risk Management both requires and contributes to strengthened partnership with contractors—whether or not there is a formal Team Risk Review. In fact, through Risk Management the segment identified a need for improved contractor information on schedules, *and* provided precise government information to request better contractor information.
- Streamlining of the Risk Management process is appropriate. Segment 32 "spun some wheels" until it clarified that the *outcomes* of Risk Management—institutionalizing Risk Management culture and awareness and being able to integrate Risk Management from the division into the system-level—were the keys.
- Advance system planning would reap important dividends on management reserve, trades along the interfaces, and creating an efficient system-wide Risk Management process. Introducing Risk Management after key decision points had been passed created unnecessary, and preventable, stress to the divisions.
- Candor and cooperation among the division chiefs is essential for system-wide Risk Management to succeed.

6.3.2.2 Segment 32 Next Steps/Recommendations

Segment 32 has a number of recommendations, especially for improving system-level Risk Management and broader dissemination across the NRO:

- *For the division: Plan a follow-up offsite meeting annually after the initial Risk Clinic/risk identification/mitigation strategy planning session.* Segment 32 plans to hold an offsite meeting to revisit and reappraise its current Risk Management process and revise it as appropriate, based on decisions by the entire Segment 32 team. At the offsite meeting, the division will also review and update its risk list and determine, based on the reorganization and new program mission, whether a full risk identification and mitigation strategy planning session should be held.
- *For the divisional level: Install the Risk Management tool "at a workstation on everyone's desk."* As a result of this, Risk Management could become not only part of everyone's consciousness but also their daily work. (This recommendation was also mentioned in the Segment 2 interview.)
- *For the system level: The government should think in terms of allocating management reserve to Risk Management—up front—when planning and launching programs.* Difficulties such as those that arose in Segment 32—lack of funding for Risk Management, and the need to negotiate late in the process with contractors to cut into their reserve for critical Risk Management activities—could thereby be prevented. (Other divisions also point to the need for disciplined inclusion of a management reserve for Risk Management into program/project management plans.)

- *For the system level: Establish the Risk Management tool and other standardized procedures, templates, and approaches from the beginning.* Don't create an artificial expectation that each division's "best practice" will be compiled and selected or integrated—as was the understanding at IDP. This approach "wasted time and energy, and disappointed people."
- *For further NRO installation of Risk Management: Articulate more clearly the methods for streamlining the process and defining relevant factors.* "Not every step of the full Risk Management process needs to be enacted in every case; guidance as to what and how to tailor would help."
- *The internal technology platform must support a system tool.* Because the technology platform was not standard across or even within divisions, the Risk Management tool was harder to install and use across the system.

6.3.3 Segment 2 Lessons Learned, Next Steps/Recommendations

6.3.3.1 Segment 2 Lessons Learned

Segment 2 has identified the following as lessons learned:

- Participation of two Segment 2 project managers in the IDP Risk Management cadre provided cross-system linkages and cooperative, ongoing inter-divisional communication on Risk Management.
- The Segment 2 division chief initially believed that the segment's Risk Management process was sufficient and questioned the wisdom of the new Risk Management processes. The value-added that was discovered was the enhanced communication on cross-divisional risks. Once this approach became standard operating procedure, this director participated actively in the ESRT.
- Though Segment 2 did not establish a formal, joint government/contractor Team Risk Review, Segment 2 perceived that contractor alignment with the government Risk Management process would be helpful and considered Risk Management training for them. Given the press of schedules, Segment 2 instead worked on a mentoring/coaching basis with contractors to bring them up to speed, and this eventually resulted in more disciplined Risk Management by the contractor.
- The system level may have made a mistake in allowing for the development of "best risk practices," which resulted in wasted effort. For example, the Segment 32 database was considered by Segment 2 for internal application, and the Risk Management tool was then approved for system standardization.

6.3.3.2 Segment 2 Next Steps/Recommendations

Segment 2 also has recommendations for system-level and NRO Risk Management, as well as for its own divisional process, including the following:

- *For the division: Continue alignment of contractor Risk Management with government Risk Management.* While this has begun, the division is exploring ways to make advances in having a successful partnership on Risk Management.

- *For system-level Risk Management: Create a communications strategy to voice the senior leader's priorities on Risk Management.* A disconnect occurred in Segment 2 between the actual sponsor priorities and divisional understanding, because the ESRT was the principal vehicle of communication about Risk Management. Segment 2 recommended that there be consistent and clear emphasis on Risk Management throughout all system-level meetings and planning sessions.
- *For system-level Risk Management: Find a methodology to facilitate cross-divisional and system-level comparisons.* Attribute criteria has been confusing—cross-divisional and system-level comparisons have been difficult.
- *For future installation of Risk Management at the NRO: Define more clearly the existing practices; establish criteria for a fully executed Risk Management process and assess against that.* In partnership with the divisions, identify as precisely as possible existing practices in both Risk Management and program management, and then define the gaps that need to be filled.
- *For future installation of Risk Management at the NRO: Define upfront the tools and approaches that will be standardized.* Formulate clearly where tailoring is appropriate and essential to Risk Management, and where standardization is appropriate and essential.

6.4 Summary of Knowledge Management

The project with IMINT/EIS is a full SEI Risk Management implementation, now in its second full year. The implementation has required that managers substantially alter the way they do their jobs. Resistance to the changes brought about by Risk Management has been one of the thorniest problems related to the implementation. That problem has been made more difficult by the culture of IMINT/EIS, which reflects the culture of the NRO in general. NRO is of necessity a highly secretive organization; its existence was not officially acknowledged until very recently. As such, open communication—albeit internal communication—requires that some work be done to change the culture. Information sharing is a challenge among various groups and with those from outside the organization, such as the Risk Management implementation team.

In addition, Acquisition Risk Management is an SA-CMM key process area at Level 3. This is significant in that a certain level of organizational maturity in a complex, interlocking set of capabilities is a necessary platform for fully robust Risk Management to be executed. At the same time, Risk Management supports organizational maturation. However, there were a number of key practices that had yet to be installed at IMINT that were critical for ongoing development of a fleet, agile, and mature process-based organization.

Still, based on the perspective of many people involved with Risk Management, both the system-level and the divisions achieved real accomplishments. While there remains the challenge of full incorporation of Risk Management into business operations, the groundwork has been laid and it can be built upon.

Lessons learned from the past two years can be of value for ongoing and new Risk Management efforts. The primary lessons learned from the implementation can be broadly captured in the following categories:

- *There will be cultural resistance.* In a reluctant—if not hostile—organization, it can be helpful to first make inroads with a pilot program.
- *Risk Management must be implemented at the systems level.* Although a pilot can help open the door, Risk Management must be implemented system-wide.
- *Implementers must reach a critical mass of cooperation.* It might not be necessary to obtain 100 percent cooperation in order to achieve significant core results in Risk Management. Implementers should try to establish a critical mass of support and cooperation.
- *Sequence is important.* The sequence in which groups go through the steps of Risk Management (training, Risk Clinics, etc.) is important. In particular, implementers should strongly encourage organizations to begin with training. Failure to do so will likely result in backtracking and delays.
- *The process is tailorable.* The Risk Management effort can be tailored for various parts of an organization. Ultimately, however, risk information must be delivered to upper management in a standardized form.
- *Tool and process go hand-in-hand.* The system Risk Management tool is highly valuable for supporting system Risk Management processes, but the government process itself, active within and across divisions, is the critical success factor for proactive Risk Management.
- *Implementers should maintain contact.* The implementation team should maintain constant contact with the implementing organization.
- *Contractors might have other interests.* In a government/contractor relationship, governmental organizations should recognize that contractors may not always share their interests. Contractors are motivated by the need to maintain a business relationship while government is motivated by the need to deliver the final product.
- *Government and contractors are partners, with the government having ultimate program accountability.* Effective government/contractor partnerships are the core of effective Risk Management in an acquisition-intensive organization. Concurrently, while contractor Risk Management and government/contractor partnerships are essential, the government must retain the ultimate accountability for program results, and therefore, for ownership and guidance for program Risk Management.
- *Champion support is critical.* By earning the support of the manager of the software engineering group, the implementation team gained a key champion, credibility, and momentum.
- *Risk Management requires culture change and culture management.* It is always easier to revert to paying attention to near-term, present problems rather than thinking forward to prevent or reduce downstream risks—with the result that problems accumulate and accelerate further. Continuous Risk Management needs to become "in the drinking water," yet entails periodically renewed commitment to ensure the "way we do business" includes the business of Risk Management.

- *Visible, committed, ongoing sponsorship by senior management is the most important factor for Risk Management success.* Solid sponsorship is needed, from dedicating resources for Risk Management installation to assuring that risks are continuously discussed, identified, planned, and tracked to serious consideration of mitigation proposals with requests to fund mitigation plans. Sponsorship remains important at every step of the way.

7 Conclusion

We believe this technical report provides a rich example of a Risk Management implementation that was objectively initiated, evaluated, sustained, and installed in an organization going through significant change in all areas: mission, staff, and facilities.

We have endeavored to exhibit how the NRO's management, recognizing the composite of new challenges before it, focused on major fundamental improvements in how it conducted its business. The new paradigm of divesting system responsibilities among mission partners and the requisite need for an unparalleled level of cooperation and meshing of divergent program constraints taken all at once could have been debilitating. Instead the NRO leadership embarked upon a steady, disciplined approach to changing its basic business paradigm.

Using the results of the Software Acquisition Capability Maturity Model assessment in conjunction with other external studies (such as Malcolm Baldrige award criteria), NRO management developed a focused Risk Management program that encompassed one of its major technical programs, the Enhanced Imagery System within the Imagery and Intelligence (IMINT) directorate. This was accomplished by selecting a pilot division and allowing that pilot to benefit and capitalize upon the improvement investment or not. Dissolution of the effort was known to be an acceptable result, if the managers of the pilot were so inclined. However, the pilot instead showed value and managers eagerly embraced the Risk Management concepts and principles published by the Software Engineering Institute's Risk Management Program. From this successful pilot the IMINT/EIS director launched a directorate-wide implementation program that was to be completed within nine months. These objectives were met, not without some stumbles, but ultimately with some significant successes. The essential Risk Management paradigm of identify, analyze, plan, track, control and communicate provided the organization with a process and a vocabulary that has enabled more project management and less "crisis management." The principles of global perspective, shared product vision, forward-looking view, teamwork, integrated management, continuous process, and the core principle of open communication have been applied collaboratively with the EIS contractors. The risk evaluations, Team Risk Reviews, Continuous Risk Management training, and Risk Clinics, as well as the EIS Individual Development Program's Oracle-developed tool, the Risk Management tool, have been delivered, are visible, and have been explicitly enacted by most of the EIS directorate Individual Development Programs (IDPs) and their contractors.

Finally, this technical report tells the story of the NRO/IMINT Risk Management rollout. We have exposed the facts of the implementation rollout. We have also shared the individual IDP

managers' viewpoints and perspectives, as well as those of their contractors, that were encountered along the way. Generally, this was a story of persistence toward a goal of making fundamental improvements in the way the IMINT/EIS IDPs were managed, and the achievement of that goal. Fundamental improvements were implemented and, to date, have been declared successful. This achievement was one of significant collaboration among the IMINT/EIS IDPs, their respective managers, and their contractors. It is expected that these practices will be absorbed into the evolving business-process improvement initiatives ongoing at the NRO.

We have provided many examples of where the Risk Management process worked and some where it didn't, but in all cases the success or failure was known. The number of surprises was significantly reduced and more disciplined program management eventually became the norm.

The following are highlights of the lessons learned:

- Build Risk Management into the program management/system management structure at the beginning.
- You will have cultural resistance. Plan for it.
- Constancy of management support and an internal champion are musts.
- Contractor buy-in and collaboration enhances the adoption of Risk Management as a business process.
- Define all roles explicitly.
- Provide a consistent set of tools and ensure their continuous use.

Bibliography

[Air Force 88]	Air Force Systems Command/Air Force Logistics Command Pamphlet 800-45. Software Risk Abatement, September 30, 1988.
[Air Force 95]	Department of the Air Force, Software Technology Support Center. *Guidelines for Successful Acquisition and Management of Software Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems Volume 1, Version 1.1*. Salt Lake City, Utah: Department of the Air Force, Software Technology Support Center, 1995.
[Akao 90]	Akao, Yoji. *Quality Function Deployment: Integrating Customer Requirements into Product Design*. Cambridge, MA: Productivity Press, 1990.
[Baker 94]	Baker, Emanuel R.; Cooper, Lee; Corson, Barry A.; & Stevens, Arthur E. "Software Acquisition Management Maturity Model (SAM3)." *Program Manager*, July–August 1994.
[Bell 89]	Bell, Trudy E. "Managing Murphy's Law: Engineering a Minimum-Risk System." *IEEE Spectrum*, 26, 6 (June 1989): 24–27.
[Boehm 89]	Boehm B. *IEEE Tutorial on Software Risk Management*. New York: IEEE Computer Society Press, 1989.
[Boehm 91]	Boehm, Barry W. "Software Risk Management: Principles and Practices." *IEEE Software*, 8, 1 (January 1991): 32–41.
[Brooks 87]	Brooks, Fred P. "No Silver Bullet: Essence and Accidents of Software Engineering." *IEEE Computer* 20, 4 (Apr. 1987), 10-19.
[Carr 93]	Carr, Marvin; Konda, Suresh; Monarch, Ira; Ulrich, Carol; & Walker, Clay. *Taxonomy-Based Risk Identification*. (CMU/SEI-93-TR-6, ADA266992). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1993. <URL: http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr06.93.pdf>

[CCTA 94]	*Management of Project Risk*. London, UK: CCTA, 1994.
[Charette 89]	Charette, Robert N. *Software Engineering Risk Analysis and Management*. New York, NY: McGraw-Hill, 1989.
[Charette 90]	Charette, Robert N. *Application Strategies for Risk Analysis*. New York: Multiscience Press, 1990.
[Chittister 93]	Chittister, Clyde; & Haimes, Yacov Y. "Risk Associated with Software Development: A Holistic Framework for Assessment and Management." *IEEE Transactions on Systems, Man, and Cybernetics*, 23, 3 (May-June 1993):710-23.
[Clark 95]	Clark, Bill. "Technical Performance Measurement in the Risk Management of Systems," Presented at the Fourth SEI Conference on Software Risk, Monterey, CA, November 6-8, 1995. For information about how to obtain copies of this presentation, contact SEI Customer Relations at (412) 268-5800 or Internet: customer-relations@sei.cmu.edu.
[Coulter 95]	Coulter, Neal; Monarch, Ira; Monarch, Suresh; & Carr, Marvin. *An Evolutionary Perspective of Software Engineering Research Through Co-Word Analysis* (CMU/SEI-95-TR-019, ADA 309159). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1995. <URL: http://www.sei.cmu.edu/pub /documents/95.reports/pdf/tr019.95.pdf>
[Deming 82]	Deming, W. Edward. *Out of the Crisis*. Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study, 1982.
[Dorofee 96]	Dorofee, Audrey J.; Walker, Julie, A.; Alberts, Christopher J.; Higuera, Ronald P.; Murphy, Richard L.; & Williams, Ray C. *Continuous Risk Management Guidebook*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996.
[DSMC 86]	Defense Systems Management College. *Risk Management: Concepts and Guidance*. Fort Belvoir, VA: DSMC, 1986.
[Ferguson 96]	Ferguson, Jack; Cooper, Jack; Falat, Michael; Fisher, Matthew; Guido, Anthony; Marciniak, John; Matejceck, Jordan; & Webster, Robert. *Software Acquisition Capability Maturity Model® (SA-CMM®).Version 1.01* (CMU/SEI-96-TR-020, ADA 320606). Pitts-

	burgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996. <URL: http://www.sei.cmu.edu/pub/documents /96.reports/pdf/tr020.96.pdf>
[FitzGerald 90]	FitzGerald, Jerry; & FitzGerald, Ardra F. "A Methodology for Conducting a Risk Assessment." *59-72 Designing Controls into Computerized Systems*. 2nd ed., Redwood City, CA: Jerry FitzGerald & Associates, 1990.
[Gallagher 97]	Gallagher, Brian P.; Alberts, Christopher A.; Barbour, Richard E., *Software Acquisition Risk Management Key Process Area (KPA), A Guidebook Version 1.0* (CMU/SEI-97-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. <URL: http://www.sei.cmu.edu/pub/documents/97.reports /pdf/97hb002.pdf>
[Gluch 94]	Gluch, David P. *A Construct for Describing Software Development Risks* (CMU/SEI-94-TR-14, ADA284922). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1994. <URL: http://www.sei.cmu.edu/pub/documents/94.reports /ps/tr14.94.ps>
[Gluch 95]	Gluch, David P.; Dorofee, Audrey J.; Hubbard, Elizabeth A.; & Travalent, John J. *A Collaboration in Implementing Team Risk Management* (CMU/SEI-95-TR-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1995. <URL: http://www.sei.cmu.edu/pub/documents/95.reports /pdf/tr016.95.pdf>
[Haimes 93]	Haimes, Yacov Y.; & Chittister, Clyde *Acquisition Process for the Management of Risks of Cost Overrun and Time Delay Associated with Software Development* (CMU/SEI-93-TR-28, ADA276466). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1993.
[Henley 92]	Henley, Ernest J.; & Kumamoto, Hiromitsu. *Probabilistic Risk Assessment*. New York, NY: IEEE Press, 1992.
[Higuera 93]	Higuera, Ronald P. & Gluch, David P. "Risk Management and Quality in Software Development." Proceedings of the Eleventh Annual Pacific Northwest Software Quality Conference. Portland, Oregon, October 18-20, 1993. Portland, Oregon: Pacific Northwest

	Software Quality Conference, 1993.
[Higuera 94a]	Higuera, Ronald P.; Dorofee, Audrey J.; Walker, Julie A.; & Williams, Ray C. *Team Risk Management: A New Model for Customer-Supplier Relationships* (CMU/SEI-94-SR-05, ADA283987). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1994. <URL: http://www.sei.cmu.edu/pub/documents/94.reports/pdf/sr05.94.pdf>
[Higuera 94b]	Higuera, Ronald P.; Gluch, David P.; Dorofee, Audrey J.; Murphy, Richard L.; Walker, Julie A.; & Williams, Ray C. *An Introduction to Team Risk Management* (CMU/SEI-94-SR-01). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, May 1994. <URL: http://www.sei.cmu.edu/pub/documents/94.reports/pdf/sr01.94.pdf>
[Higuera 96]	Higuera, Ronald P.; & Haimes, Yacov. *Software Risk Management* (CMU/SEI-96-TR-012, ADA 315789). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1996. <URL: http://www.sei.cmu.edu/pub/documents/96.reports/pdf/tr012.96.pdf>
[Jones 93]	Jones, Capers. *Assessment and Control of Software Risks.* Englewood Cliffs, NJ: Yourdon Press, 1993.
[Juran 88]	Juran, J.M. *Juran's Quality Control Handbook: Fourth Edition.* New York, NY: McGraw Hill Book Company, 1952, 1979, 1988.
[Juran 89]	Juran, J.M. *Juran on Leadership for Quality.* New York, NY: The Free Press, A Division of Macmillan, Inc., 1989.
[Kaplan 81]	Kaplan, Stanley; & Garrick, John B. "On The Quantitative Definition of Risk." *Risk Analysis*, 1, 1, (1981): 11-27.
[Karolak 96]	Karolak, Dale Walter. *Software Engineering Risk Management.* Los Alamitos, Calif.: IEEE Computer Society Press, 1996.
[Katzenbach 93]	Katzenbach, Jon R.; & Smith, Douglas K. "The Discipline of Teams." *Harvard Business Review*, 72, 2 (March-April, 1993): 111-120.
[Kezsbom 89]	Kezsbom, Deborah S.; Schilling, Donald L.; & Edward, Katherine A. *Dynamic Project Management.* New York, NY: John Wiley &

	Sons, 1989.
[Kirkpatrick 92]	Kirkpatrick, Robert J.; Walker, Julie A.; & Firth, Robert. "Software Development Risk Management: An SEI Appraisal." *Software Engineering Institute Technical Review '92* (CMU/SEI-92-REV). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1992.
[Krum 00]	Krum, Al; Neitzel, August C.; Loveland Link, Jo Lee; & Barbour, Rick. "Risk Management Rollout and Installation at the National Reconnaissance Office." *CrossTalk: the Journal of Defense Software Engineering*. Hill Air Force Base, Utah: Ogden ALC. February 2000.
[Loveland Link 99]	Loveland Link, Jo Lee; Barbour, Rick; Krum, Al; & Neitzel, August C., Jr. *Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office* (CMU/SEI-99 TR-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999.
[Michaels 96]	Michaels, Jack V. *Technical Risk Management*. Upper Saddle River, NJ: Prentice-Hall, 1996.
[Modarres 93]	Modarres, M. (Mohammad). *What Every Engineer Should Know About Reliability and Risk Analysis*. New York, NY: M.Dekker, 1993.
[Monarch 95]	Monarch, Ira; & Gluch, David P. *Experiment in Software Development Risk Information Analysis* (CMU/SEI-95-TR-014, ADA 302320). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1995. <URL: http://www.sei.cmu.edu/pub /documents/95.reports/pdf/tr014.95.pdf>
[Neitzel 99]	Neitzel, August C., Jr. "Managing Risk Management." *CrossTalk: the Journal of Defense Software Engineering*. Hill Air Force Base, Utah; Ogden ALC, July 1999.
[NRC 89]	Committee on Risk Perception and Communication, Commission on Behavioral and Social Sciences Education, National Research Council. *Improving Risk Communication*. Washington, D.C.: National Academy Press, 1989.
[Rowe 88]	Rowe, William D. *An Anatomy of Risk*. Malabar, Fla.: Robert E.

	Krieger, 1988.
[Saaty 80]	Saaty, Thomas L. *The Analytic Hierarchy Process*. McGraw-Hill, Inc. 1980.
[Scarff 93]	Scarff, Frances. *An Introduction to the Management of Risk*. London, UK: CCTA, 1993.
[Scholtes 88]	Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality*. Madison, WI: Joiner Associates, Inc., 1988.
[SEI 92]	Software Engineering Institute. "The SEI Approach to Managing Software Technical Risks." *Bridge* (October 1992): 19-21. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1992.
[Sisti 94]	Sisti, Frank J. & Joseph, Sujoe. *Software Risk Evaluation Method Version 1.0* (CMU/SEI-94-TR-19, ADA290697). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1994. <URL: http://www.sei.cmu.edu/pub/documents/94.reports/pdf/tr19.94.pdf>
[Van Scoy 92]	Van Scoy, Roger L. *Software Development Risk: Problem or Opportunity* (CMU/SEI-92-TR-30, ADA258743). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1992. <URL: http://www.sei.cmu.edu/pub/documents/92.reports/pdf/tr30.92.pdf>

Glossary[14]

Accountability — Defines who must ultimately answer for the success or failure of managing a risk.

Analyze — Define attribute criteria: impact, probability, timeframe. Classify risks to group, consolidate and enhance decision making. Prioritize risks to determine which will receive the most focused attention.

Attribute — Risk attributes include probability of occurrence, impact, and timeframe. Each attribute has specific criteria to characterize it as high, medium, or low.

Condition — Description of the key circumstances situations, etc., that cause concern, doubt, or uncertainty.

Consequence — Description of key possible negative outcome(s) of the current conditions.

Context — Context provides additional detail regarding the events, circumstances, and interrelationships within the project that may affect the risk or mitigation plan. This description is more detailed than can be captured in the basic statement of risk.

Contingency plan — In tracking a risk mitigation plan, a predetermined threshold or trigger may indicate that the mitigation plan is not effective, and that a contingency plan for corrective action is necessary. In this case the risk and its original mitigation continue to be tracked.

Continuous Risk Management — Continuous Risk Management is a *software engineering (acquisition) practice* with processes, methods, and tools for managing risks in a project in an ongoing way. It provides a disciplined environment for proactive decision making to

- assess continuously what could go wrong (risks)
- determine which risks are important to address

[14] From Case, Pam & Loveland Link, Jo Lee. *A Guidebook for IDP Risk Management Practitioners.* Pittsburgh, PA: Software Engineering Institute, 1999.

- implement strategies to deal with those risks

Control

One of the six functions of the SEI Risk Management paradigm. The *control* function is a process that takes the tracking status reports for the watched and mitigated project risks and decides what to do with them based on the reported data. The accountable person for a risk normally makes the control decision for that risk. The general process of controlling risks includes

- analyzing the status reports
- deciding how to proceed
- executing the decisions

ESRT

EIS System-Level Risk Team. This group addresses system-level risks that may be submitted directly to this level or may be transferred from a division-level risk process.

Identify

One of the six functions of the SEI Risk Management paradigm. The *identify* function is a process of transforming uncertainties and issues about the project into distinct (tangible) risks that can be described and measured. Identifying risks involves two activities:

1. capturing a statement of risk
2. capturing the *context* of a risk

Impact

The loss or effect on the project if the risk occurs. Impact is one of the three attributes of a risk.

Infrastructure costs

Those costs associated with implementing Risk Management activities and supporting Risk Management processes, methods, and tools within the organization. These costs may be spread out across multiple projects.

Measure (metric)

A standard way of measuring some attribute of the Risk Management process. Risk and mitigation plan measures can be qualitative or quantitative. Measure is synonymous with metric.

Mitigation checklist

A simple type of mitigation plan, this is a simple list of actions, responsibility, and due dates for completing the actions associated with a mitigation strategy.

Mitigation costs

The costs directly associated with mitigating specific risks to the project. This is the cost of carrying out the mitigation plan.

Mitigation plan

A plan for risks that are to be mitigated. It documents the strategies, actions, goals, schedule dates, tracking requirements, and all other supporting information needed to carry out the mitigation strategy. A more detailed task plan may be used for complex risks or sets of risks, or complex, expensive mitigation plans that require extensive details relevant to scheduling, budgets, actions, contingency plans, task interrelationships and dependencies, etc.

Open communication

The core principle of Continuous Risk Management, *open communication* requires

- encouraging free-flowing information at and between all project levels
- enabling formal, informal, and impromptu communication
- using consensus-based and other open processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk)

Probability

The likelihood that a risk will occur. *Probability* is one of the three attributes of a risk.

Risk approach

The course of action chosen for dealing with a risk. This can be

- a *research plan* (for risks that need to be analyzed or researched)
- an *acceptance rationale* (for risks that are accepted)
- *tracking requirements* (for risks that will be watched)
- a *mitigation plan* (for risks that will be mitigated)
- *watching* and monitoring risk attributes for significant changes

Risk baseline

A "snapshot" of all currently known risks to a project, used to begin the process of implementing Risk Management.

Timeframe

In Risk Management, *timeframe* is the period in which action must be taken.

Track

One of the six functions of the SEI Risk Management paradigm. *Tracking* includes acquiring, compiling, and reporting data indicators for triggers, thresholds, and contingency plans.

Transfer

To allocate *authority*, *responsibility*, and *accountability* for a risk to another person or organization. This is considered a lateral or upward transition of responsibility—e.g., to a customer or another

team in the organization.

Trigger

Thresholds for *indicators* that specify when an action, such as implementing a contingency plan, may need to be taken. *Triggers* are generally used to

- provide warning of an impending critical event
- indicate the need to implement a contingency plan to preempt a problem
- request immediate attention for a risk

Appendix

A.1 Managing Risk Management

The following article by August C. Neitzel, Jr., appeared in the July 1999 issue of *CrossTalk: The Journal of Defense Software Engineering,* Hill Air Force Base, Utah: Ogden ALC, July 1999.

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 Ac-

quisition-Capability Maturity Model℠ (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.

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.

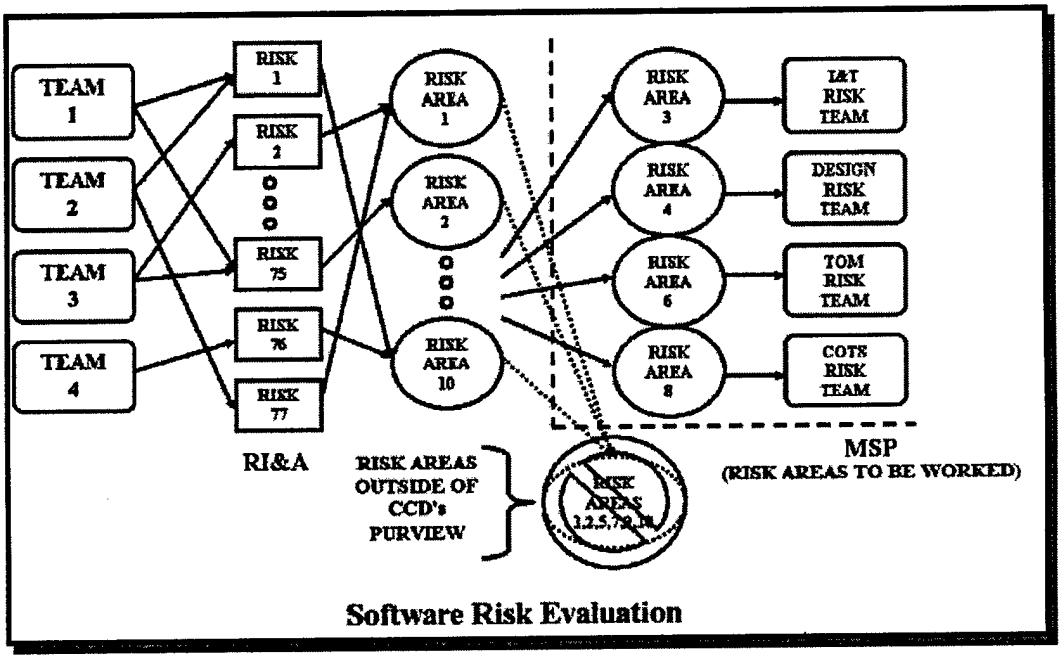


Figure 1. Software risk evaluation process.

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 taking 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.

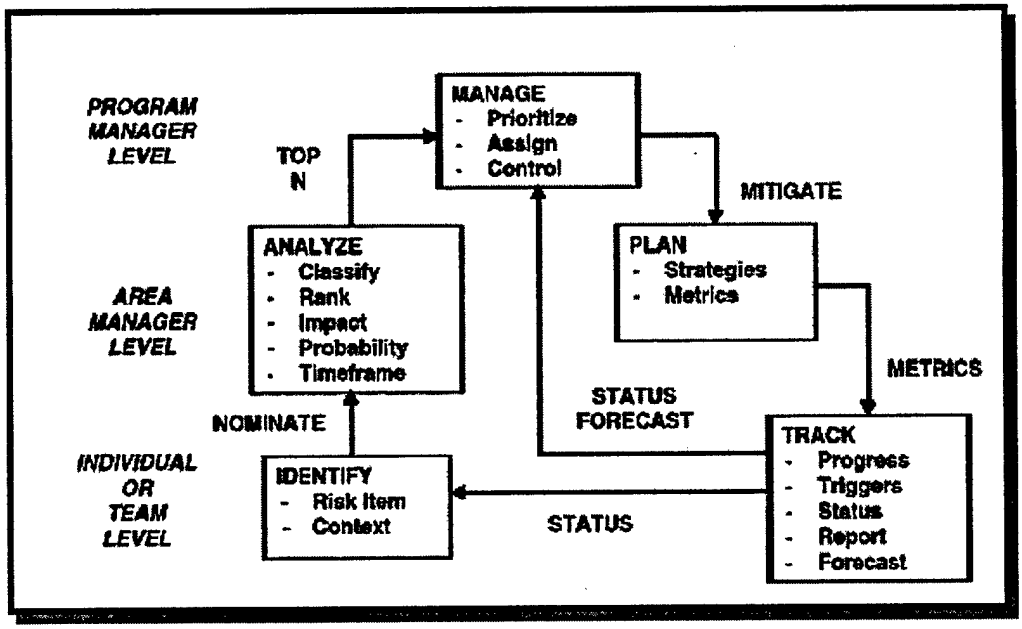


Figure 2. Continuous risk management flow.

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.

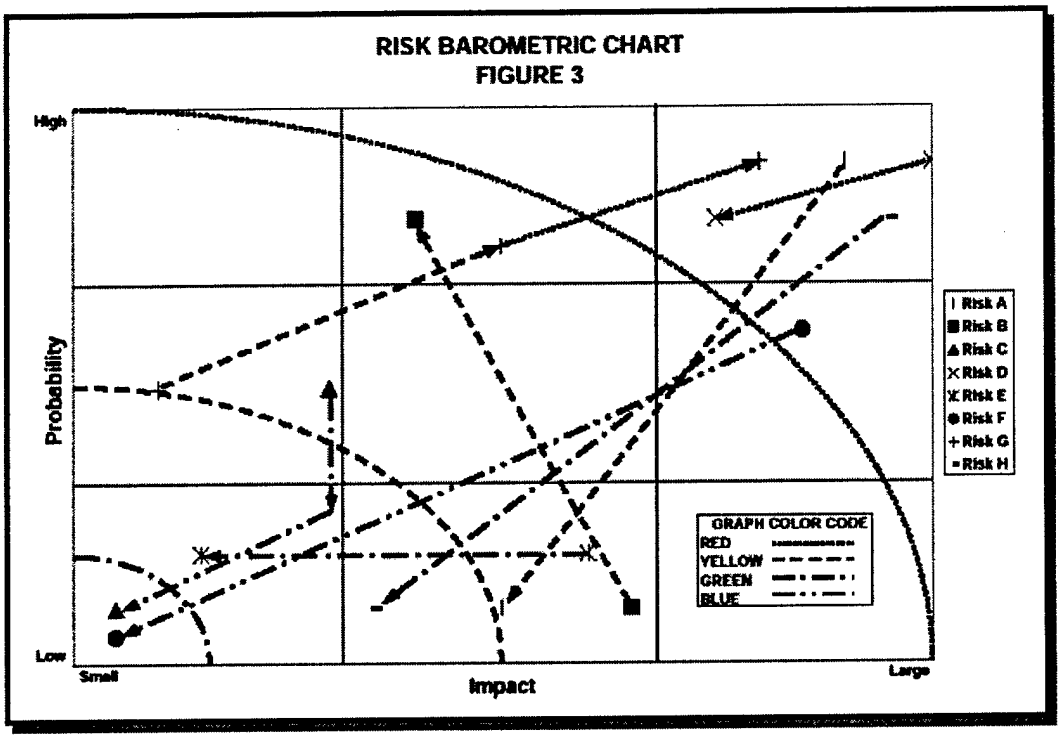


Figure 3. Risk barometric chart.

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" category for IMINT at large.

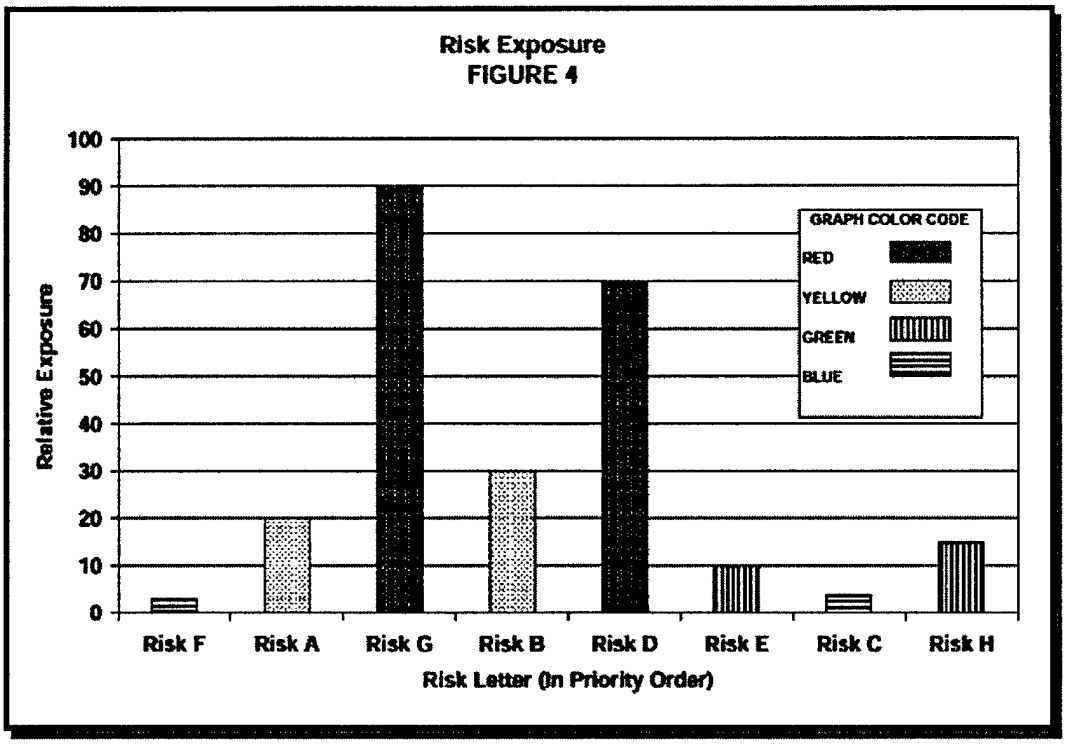


Figure 4. Risk exposure.

(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.

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

References

1. Software Acquisition-Capability Maturity Model (SA-CMM) V1.01 (CMU/SEI-96-TR020)

2. *Continuous Risk Management Guidebook*, CMU/SEI, October 1996.

A.2 Encouraging Winning Risk Management Behavior: The Exercise Left to the Student

The following article by Art Gemmer and Philip Koch appeared in *Proceedings of the 1997 SEI Conference on Risk Management*, "Managing Uncertainty in a Changing World," April 7–9, 1997, Virginia Beach, VA.

Encouraging Winning Risk Management Behavior:
The exercise left to the student

Art Gemmer & Philip Koch
Rockwell

Columnist Dave Barry writes of a group of engineers trying to improve the process of lighting charcoal grills.[1] After numerous attempts involving hair dryers, vacuum cleaners, propane torches and acetylene torches they hit upon the idea of using liquid oxygen to speed the process. Several gallons of liquid oxygen were poured over sixty pounds of charcoal and ignited. The resulting fireball consumed two-thirds of the charcoal and three seconds later the remaining charcoal was ready for grilling. Unfortunately the grill had been vaporized in the process. These people had lost site of the result they wanted to achieve.

What is the result we desire from risk management? Risk consists of three components: choice, probability and impact.[2] Of these, choice is the key component since it is the one we control. Effective risk management within an organization means the organization makes better choices. And organizations make thousands of choices every day. Virtually everything managers and engineers do is make choices. They make cost and schedule commitments, assign resources, tailor processes, make design tradeoffs, select algorithms and so on. Lots of big and little choices. And the outcome of each choice carries some amount of uncertainty. While assigning a risk analyst to concentrate on "big decisions" will provide some benefit, big decisions don't always seem big at the time they are made. So, effective risk management can't be limited to a select few.

Effective risk management requires three elements:[3]

- A repeatable process
- Widespread access to adequate sources of knowledge
- Functional behavior (supportive, as opposed to dysfunctional)

Much has been written about the elements of risk management. So why do so many organizations have trouble implementing risk management as a formal practice? It is in large part because they, like our outdoor chefs, don't focus on the result they are trying to achieve.

Current literature focuses on the first of these elements. Read just about any book on risk management and it will describe processes, methods, tools, taxonomies, checklists, tables, forms and formats. The literature is also beginning to address the second element, knowledge management, in the form of risk or data warehouses. Although each of these elements is essential to effective risk management, our experience is that the third element, functional behavior, is the key. It is the element closest to the result we desire (making better

choices). It is also the least well understood. What has been written about it focuses on discouraging dysfunctional behavior' rather than encouraging functional behavior and functional behavior is not the direct converse of dysfunctional behavior. Functional behavior is therefore not a necessary consequence of eliminating dysfunctional behavior. Just because we don't "shoot the bearer of bad news" doesn't mean we know
how to have a meaningful discussion of the news. Functional behavior also is not a necessary consequence of following a repeatable or providing widespread access to adequate sources of knowledge. The processes and methods for risk management are relatively simple when compared to those of say, software development, yet few organizations have been able to successfully implement effective risk management using them. Following a repeatable process may mean we are just systematically managing risk poorly. Having adequate sources of knowledge available doesn't necessarily motivate people to use them. That a repeatable process and adequate knowledge sources is not enough can be seen in some recent, well-publicized failures such as Metallgesellschaft Refining & Marketing (MGRM).[3] However, achieving functional behavior, a "risk taking ethic"[5], can encourage people to use a repeatable process and seek out additional sources of knowledge.

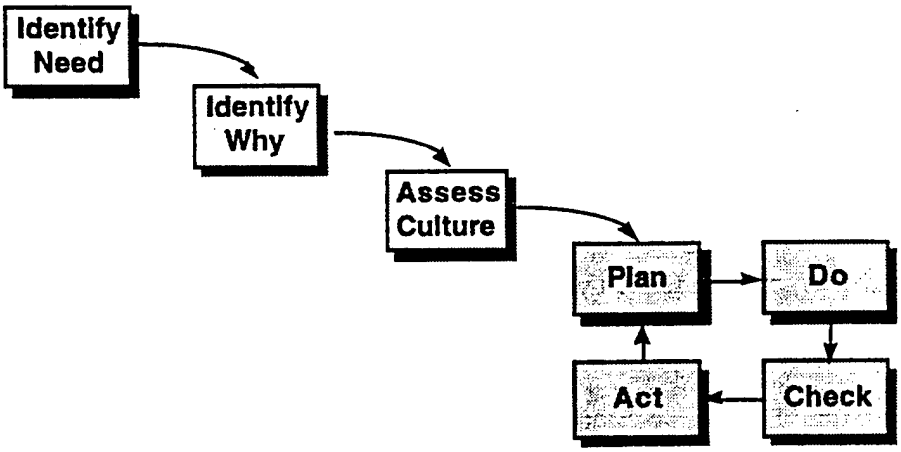


Figure 1. The Learning Model

All of us remember a time in school when our teacher worked through the simple part of a difficult problem only to leave the remainder as an "exercise to the student". Current risk management literature gives us the first part of the problem. Recognizing and encouraging functional behavior is the exercise left to the student.

DYSFUNCTIONAL BEHAVIORS. Although dysfunctional behaviors are not the converse of functional behaviors, they do offer clues as to what the functional behaviors are. They also define the gap between current and desired behavior.

Rockwell has used an approach called the Learning Model[6] to focus on behavioral aspects of cultural change. The Learning Model is the classic Plan-Do-Check-Act cycle preceded by three steps. The purpose of these additional steps is to create a "pull" for the change being introduced and to understand the cultural issues that could stand in the way of its effective implementation. Although these steps could be considered a part of the initial planning step, their importance has been found to be so critical to successful change initiatives they are identified separately. A cultural assessment was performed before implementing change in our organization's risk management practices. Fifty one-on-one confidential interviews were conducted with managers ranging from the vice presidents to a sampling of first line managers, program managers and technical directors. Jefferson Davis Associates, a

marketing research firm, analyzed the interview data. They had just completed an analysis of Rockwell's biannual Employee Survey which covers topics including internal communications, empowerment, trust and job satisfaction. It was felt that a correlation may exist between these issues and the cultural issues that could effect successful risk management. Jefferson Davis Associates included the Employee Survey data as part of their analysis of the risk management interview data. This led to the identification of the cultural rules shown in Table 1.

Specific dysfunctional behaviors were identified for each rule by observing behaviors in the monthly program reviews (the Check step of the Learning Model). As you can see, *risk* was a four letter word here. Few people even used the word. Some people actually stuttered when they used the r-word. But these results are not unlike cultures of other organizations.[7]

INSTITUTING CHANGE. Twenty major programs were selected for implementation of improved risk management practices. Eighteen of the programs were already in the execution phase. They had a defined business objective, identified customers, funding and staffing and their product or system they was still in the development stage.

Table 1. Dysfunctional Behaviors

Cultural Rule	Observed Behaviors
Be risk averse.	Don't make decisions until the outcome is guaranteed. Allow options to be eliminated by the passing of time. Run risky decisions up the management chain for approval. Use unreasonable criteria for decision making. Don't reverse past decisions.
Be reactive.	Deal with symptoms, rather than root causes. Deal with the immediate and specific, rather than the systemic. Don't deal with anything until you have to. Believe the team can't fail.
Don't ask for risk information.	Shoot the messenger (bearer of bad news). "No news is good news!" "There's no evidence to the contrary." (without a concerted effort to find it) Allow people to learn what information to report by trial and error. Filter bad news out; show only good news. Argue away information that conflicts with the team's assumptions, decisions or success (group think). Assume the competition is weak or incompetent. Don't share information; it's power. Don't raise issues which might reflect poorly on upper management.
Ignore the soft stuff.	Shield engineering from the business and marketing aspects of programs. View management tasks as administrative overhead, not "real work". Deal only with technical issues and solutions. Ignore the "people" issues.

Cultural Rule	Observed Behaviors
Make decisions based on emotion, rather than logic.	Don't reach closure on difficult issues. Talk about the difficult issues, but don't document them. Discuss them regularly, covering the same ground as before. Accept silence as a sign of consensus or agreement. Don't document or follow up on decisions made.
Reward heroes.	Believe the team can't fail. Pretend programs can be made to succeed by sheer force of will. Assign the best people to crises. Reward "lone rangers". Assume engineering can pull off miracles on a regular basis. Don't forget people's failures.
Make commitments without determining the probability of success.	Accept constraints without questioning whether a feasible solution set exists. Assess probability intuitively and subjectively. Deal with estimates as point values. Don't believe estimates. Expect the last best performance. Always plan for the best case scenario.
Don't bring forward risks or problems without solutions.	Expect problems and risks to be brought forward "already solved". Think of risks as something that can be solved. Don't delegate upwards. Micromanage or burden with the messenger with tasks.

The risk management process used at Rockwell is not much different from others described in the literature. It is supported by methods such as Risk Taxonomies, Interrelationship Digraphs and Isorisk Charts. Three types of artifacts are used by each program to capture risk information. They are:

- *Impact Model:* Establishes "pain thresholds" for variances in program performance against the program's specific expectations (see Table 5). Used to quantify risk impacts on a normalized scale (0.0 to 1.0), establish priorities and apply boundary conditions for reporting.

- *Risk Watch List:* Identifies priorities for risks meeting the boundary conditions for reporting in program reviews.

- *Risk Template:* Identifies a risk's characteristics and the action plan for managing it.

On the risk template, each risk is characterized in terms of its:

Table 2. Risk Characteristics

Characteristic	Description
Root Causes	The detailed data and contextual information that serves as evidence of the existence of the risk.
Impact	The nature (cost, schedule, customer satisfaction, etc.) and magnitude of the consequences of a risk.
Probability	The likelihood that the consequences of a risk will be realized given that the current situation is allowed to continue.
Time Frame	The period of time during which the proactive choices associated with a risk may be exercised. Past this point, choices will begin to be eliminated simply by the passing of time.
Coupling	The effect a risk's occurrence would have on other risks or opportunities. When a risk becomes a problem it may increase the probability of other risks, increase their impact, limit the choices for dealing with them or reduce the time frame for making choices about them.

Six hours of training is provided for all program managers and technical directors. Two thirds of the training deal with the mechanics of the risk management process and one third with the behavioral aspects of risk management. Biases in perceiving risk' are addressed in training. Training begins with senior management to ensure consistency of expectations. The training is followed by workshops and one-on-on feedback sessions with specific program teams. Workshops are conducted with to assist program in the application of specific process steps and methods. An internal web site was constructed to make available information to support risk management.

Programs were asked by senior management to present their risk information in their monthly program reviews. A risk analyst was present at each review to evaluate the program's process and observe the behaviors exhibited in the review. This represents the "Do" and "Check" steps of the Learning Model. The evaluation is not a "grade" of the program manager and technical director. Rather it is an evaluation of comi2anXs effectiveness in managing risk on a specific program. Programs also receive a score based on process and behavioral criteria. The behavioral criteria accounts for about half of the total score. Programs are deemed to be following a repeatable risk management process when they average a score of 90% or more for the past four months. This level of performance must then be maintained through the end of program execution.

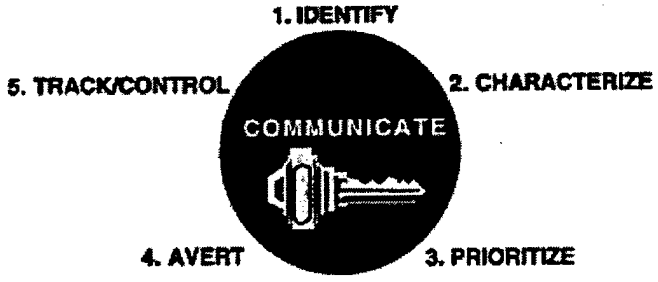


Figure 2. Rockwell's Risk Management Process

Feedback represents the "Act" step of the Learning Model. Program scores and general feedback is provided to senior management and to the programs once a month through the risk management web site. Senior management receives a monthly briefing on the status of the risk management program. Programs receive specific confidential feedback upon request.

DEFINING FUNCTIONAL BEHAVIOR. Initially, programs weren't effective at risk management even when few dysfunctional behaviors were exhibited. It wasn't just a matter of eliminating dysfunctional behavior. It mattered what behavior it was replaced with. Functional behaviors were identified by applying risk principles to variations in the observed behaviors. The dysfunctional behaviors served as a starting point. Table 3 shows the relationship between functional and dysfunctional behaviors. Because these behaviors are based on observations, they have evolved over the past year and will continue to be refined in the future.

Most of the dysfunctional rules are things people "don't do". Assuming the converse behavior to be functional may be incorrect or the converse may be an inadequate description of the functional behavior. For example, the converse of "Be risk averse" could be "Make snap decisions", but this hardly the behavior we want to encourage. The opposite of "Make decisions based on emotion, rather than logic" would be "Make decisions based on logic, rather than emotion", but it is possible to be logical without paying attention to details or attaining a common perspective. In the case of "Reward heroes", the functional behavior is to redefine a "hero" to include more than just problem solving. These distinctions may seem subtle, but they are important ("Be careful what you wish for, you may get it").

Much of the functional behavior involves reaching consensus and the consideration of multiple perspectives and information sources. Therefore, the ability to meaningfully discuss risk information is a critical skill.

Table 3. Functional Versus Dysfunctional Behaviors

Dysfunctional behavior	Functional behavior(s)
	action, even if the risks become problems in spite of our best efforts. Reward some heroes since some risks will still become problems in spite of our best efforts. Do not reward people who solve problems they knew about as risks and chose to ignore them.
Make commitments without determining the probability of success.	Track the uncertainty in performance to commitments. Manage the uncertainty in estimates. Deal with estimates as probability distributions. Plan for variations in performance. Plan for multiple scenarios, not just the best case.
Don't bring forward risks or problems without solutions.	Don't expect risks to be "solved" since some uncertainty will exist even after action has been taken to avert the risk.
View uncertainty as a negative.	Manage risk as an asset.
Treat decision making as an invariant ability of each person.	Risk management is the enabling technology for decision making.

Discussing Risk. Conducting a meaningful discussion of risk means focusing on *what* is discussed, *how* it is discussed and *what is done* as a result. At first programs presented risk information, rather than discussing it. For those programs reluctant or unsure about how to discuss risk, senior management provides a pull for the information. They are coached to create this pull by asking questions such as those shown in Table 4.

Table 4. Creating a Pull For Risk Information

If the program says...	Senior management should ask...
"Here are our risks."	Which risks do you want us to hear? Do you need our help with any of these? Do we have consensus on the risk's characteristics? Do we have consensus on the actions to be taken?
"We're taking a calculated risk."	What calculations that led you to this approach?
"There's no change in the risks."	Why? Shouldn't they decrease over time? Are we approaching the time frame (decision point) for any of the risks? What actions are already being taken? Are they effective? Has any assistance requested been provided in a timely fashion? Are we being proactive enough? Do we need to do more or something else?
"There are no significant risks."	What techniques were used to look for them? What insignificant (non-reportable) risks are being tracked?
"The risks are being worked."	What actions are being taken? How have they affected the risks' characteristics? How many risks have been realized as problems? How many risks have been averted?

Table 4. Creating a Pull For Risk Information

If the program says...	Senior management should ask...
"The risk is reduced." or "The risk went away."	Why? What about the situation has changed? Has the probability or impact decreased? Or both? Why? If the probability decreased, what uncertainty remains? If the risk was avoided, what new risks do we face?
"There are no new risks."	What techniques were used to look for them? What expectations are still unmet? How has our situation changed? Are things getting better or worse?

To assist programs in deciding which risks to bring forward, boundary conditions were established for reporting. Risks that meet at least one of the following criteria are reported upward:

- Averting the risk requires some assistance beyond the scope of control of the program.
- The risk is best managed at a higher level (e.g., by the organization or customer).
- The risk has a significant impact.

To determine significant impact, programs develop an Impact Model. Risks with projected impacts of 0.5 or greater are considered significant and will be reported regardless of their probability or the need for assistance.

Table 5. The Impact Model

Impact	Variance in Program Performance from Expectations

Catastrophic (Impact 0.75 to 1.00)	• Cost increase of more than (State 20% of approved annual budget, or cost increase of more than $200k, whichever is less)
	• Standard (recurring) cost increase of more than (State 20% of standard cost target)
	• Third miss of a customer delivery schedule (even one day)
	• Anything that causes our customer to perform a work around such as:
	  • Our customer must do something
	  • Our customer must tell their customer
	• Must defer scope to meet a delivery schedule

High (Impact 0.50 to 0.75)	• Cost increase of more than (State 10% of approved annual budget, or cost increase of more than $100k, whichever is less) • Standard (recurring) cost increase of more than (State 10% of standard cost target) • Missing any customer delivery schedule (even one day) (Refer to major milestones/deliveries) • Failure to meet reuse goal for (State what will be reused, how, by whom and when)
Medium (Impact 0.25 to 0.50)	• Cost increase of more than (State 5% of approved annual budget, or cost increase of more than $50k, whichever is less) • Standard (recurring) cost increase of more than (State 5% of standard cost target) • Slip to internal schedule which: • Puts a another task on the critical path

Impact	Variance in Program Performance from Expectations

	• Affects the critical path for an internal delivery
	• Requires an internal work around (unplanned task)
	• Reduction in planned margins or reserves (safety net beyond that required)
	  • People or equipment (State critical skills or equipment)
	  • Performance or throughput (State operating conditions and percentage)
	  • Memory reserve (State type and percentage)

Low (Impact 0.00 to 0.25)	• Cost increase of more than (State 2.5% of approved annual budget, or cost increase of more than $25k, whichever is less) • Standard (recurring) cost increase of more than (State 2.5% of standard cost target) • Task slip which reduces margin or affects resource balancing

Impact	Variance in Program Performance from Expectations

	• Affects the critical path for an internal delivery
	• Requires an internal work around (unplanned task)
	• Reduction in planned margins or reserves (safety net beyond that required)
	  • People or equipment (State critical skills or equipment)
	  • Performance or throughput (State operating conditions and percentage)
	  • Memory reserve (State type and percentage)

Low (Impact 0.00 to 0.25)	• Cost increase of more than (State 2.5% of approved annual budget, or cost increase of more than $25k, whichever is less) • Standard (recurring) cost increase of more than (State 2.5% of standard cost target) • Task slip which reduces margin or affects resource balancing

The Impact Model is two-way communication tool. It allows programs to communicate risk impacts using an agreed upon standard for the program. It also allows senior management to establish common performance priorities for all programs within the organization.

Initially, each program developed their Impact Model from scratch. This led to the following discussion of one program's Impact Model, "We're *a big program. A $100k is a small percentage of our overall budget. That might be a catastrophic impact to* a small *program, but to us it's* a nit". Senior management's response was, *'Yes, but that's still $100k I can't spend on some other program. Above that threshold, you're size doesn't* matter'. As a result, senior management developed the organization-wide guidelines for creating Impact Models shown in Table 5.

The Devil Is In The Detail. It is contrary to American culture to deal with detail.' We are impatient and love shortcuts. We want to get on with things, *the real work,* confident that we can adapt and improvise solutions to any problems caused by our inadequate up front planning. This tendency also tempts us to gloss over the details surrounding a risky decision. But detail is necessary to effective risk management. Programs are coached that a reviewer should be able to understand 95% of the risk based on the detail provided in the template without any outside explanation.

Viewcells of risk information used in reviews suffer from a basic rule of making good presentations. That is, "Use a few bullets and talk to the details". People are reluctant to provide adequate supporting rationale for estimates of probability, impact, time frame and

other coupling. These estimates have little meaning without supporting rationale. They are difficult to communicate, gain consensus on and track over time.

One presenter showed a risk template with two supporting bullets. He then talked to the details of the risk for ten minutes. V*7hen asked why these weren't included in the template he replied, *"But it wouldn't fit* on one *slide!"* as if this violated a law of physics. When detail is not captured the reviewers each take away something different from the discussion. They hear different things. This is similar to the children's game where a group sits in a circle and passes message around the circle by whispering it in the ear of the next person in line. The resulting message bears little resemblance to the original transmission. Without capturing the details, different people are more likely to focus in on different aspects of the risk. This results in difficulty in reaching consensus and taking unified action.

The attention to detail especially important for estimates of probability. Of the three characteristics: probability, impact and time frame, it is the most difficult and complex to estimate. Estimating impacts in terms of cost and schedule variance is straightforward. Determining time frames Estimating probability requires the most attention to detail and often requires the gathering of additional data once the analysis has begun. Consequently, people often estimate the probability of a risk holistically (the overall event rather than its constituent parts) and intuitively. This induces two kinds of error in their estimates. First, different people will focus on different factors which contribute to the overall probability. This leads to wide differences in probability estimates. Secondly, intuitive estimates such as these are subject to biases that are independent of the desire of the team to meet its objectives." To avoid these forms of error, programs are coached to identify the possible event sequences and reason about the individual events and probabilities in the sequence.

Reaching Consensus. The goal of discussing a risk is to reach consensus on the risk's characteristics and the action plan for dealing with it. Often disagreements stem from different people using different reasoning or data to reach their conclusions. For this reason, the focus of discussion should be on areas of differing opinions, not common ground. This notion has been called "management as conversation" which means that "the truth (consisting of beliefs with greater validity) is more likely to emerge from a dialogue between contrary beliefs than in isolation".' The danger in "agreeing to disagree" is not just a failure to reach consensus, but that the best ideas and approaches never emerge. "Individuals rarely have both the breadth and depth to act solely on their own knowledge."'

Level of Abstraction	Can we agree on...	...using this risk information?
Highest	What to do about this situation?	Risk aversion strategy and action plan
	The evaluation of the situation?	Risk statement and risk's probability, impact, time frame and coupling
	The reasoning that lead to this evaluation?	Rationale for risk's probability, impact, time frame, risk coupling
Lowest	The data used to support the reasoning?	Root causes

Table 6. The Inference Ladder As Applied To The Discussion Of Risk

The Inference Ladder[11] is used to facilitate discussions in areas of disagreement. It applies varying levels of abstraction to focus on the pertinent risk information. At the

highest level of abstraction, the goal is to reach consensus on the choice to be made (represented by the risk's action plan). If agreement cannot be reached, the discussion moves to next level of abstraction to focus on the evaluation of the situation (represented by the risk statement and its characteristics). Disagreement at this levels moves the discussion to the analysis which led to the formulation of the risks characteristics. For example:

Person A: "I don't agree with the action to be taken on this risk." (Recognize differing opinion)

Person B: "I based my choice mainly on high probability of occurrence. Do you agree with the risk's probability?" (Move down a level of risk characteristics)

Person A: "I don't agree with the estimated probability. It's too high." (Identify area of disagreement)

Person B: "I believe the risk is highly probable because the probability is mainly driven by the likelihood the supplier will fail to deliver on time. Do you agree that is the driving factor?" (Move down a level to supporting rationale)

Person A: "I agree they may be late but we won't need the part on the delivery date so it's not as likely to impact us if they slip a little. Do you agree?" (Identify use of different rationale)

And so on...

The use of levels of abstraction keeps the conversation from wandering and helps identify the basis of the disagreement. This may lead to additional investigation and data collection.

MEASURING THE BENEFITS. Since implementing risk management we have realized better, more predictable program performance. Reviews more effective and more efficient. Program teams are empowerment. The organization is better able to manage risk as an asset. A pull has been created for improved risk management process and additional knowledge sources.

Better, More Predictable Program Performance. One senior manager said, "Because of team risk identification and discussion, risks that used to become problems, don't occur now. We find solutions. We have fewer surprises". Comparing programs' risk management evaluation scores with their Schedule Performance Index (SPI from Earned Value) has shown that programs that exhibit functional risk behavior are more likely to perform to schedule. Another senior manager: "Because of risk management and earned value, we are consistently able to meet our budgets at the organizational level. In fact, our overall budget is down 30% from a few years ago and we're doing an equivalent amount of work".

Smooth Reviews. Originally there was a concern that formal risk management would make lengthy reviews even longer. Before implementing risk management most programs presented only one or two risks. These were not their biggest risks, but the ones they felt most comfortable communicating. They were backed up with little if any detail. Their discussion accounted for less than five minutes of the review. The remainder of the review was taken up discussing other problems, risks and opportunities, they just weren't recognized as such. These discussions were largely unfocused and might be conducted again at the next review. Formal risk management made these discussions not only more effective, but more efficient.

Programs exhibiting functional risk management behaviors typically finish early and easily articulate their situation. Programs not exhibiting functional risk management behaviors typically go over their allotted time and cannot easily articulate their situation. Since the review agenda is the same for all programs this difference cannot be attributed to the topics for discussion.

Pull For Process And Knowledge Sources. Once programs get serious about implementing improved risk management practices it takes them I to 4 months to reach the 90% criteria for single month. Then it's a matter of maintaining that level of performance. It is at this point that programs start pulling for improved risk management methods and broader sources of knowledge. Two of our programs are working with Russian customers and partners and as their risk management practices became better, they became more interested in information we had on Russian business culture. This helped them identify better strategies for managing their risks. Other programs are starting to apply risk management to strategic planning.

Managing Risk As An Asset. Our senior management: "Risk management helps us do better contingency planning. We hold a risk reserve at the organizational level. We use the risk exposure of our programs to determine how much reserve to hold and when we can allocate it to new work".

Managing risk analogous to managing an organization's human resources.' We manage our human resources to ensure that the types of resources (disciplines, skill sets) and the amount of each types matches our business needs. We aren't trying to eliminate risk or pursue only low risk ventures. Risk represents a competitive advantage, a discriminator. We want to pursue higher risk ventures, but those with kinds of risks we like. We need to manage this asset so that the types and quantity of risk are appropriate to our business needs. Otherwise risk will be a wasted resource. For this to happen, risk management must start before program execution. Once in execution the expectations are "set" and risk management is aimed at managing to them.

Implementing risk management during the execution phase has pointed out to our program teams and senior management the value of managing risk before the program begins. They now see the limitations of only dealing with risk during the execution phase. It is before program execution begins, before the expectations are set that the choices are available to manage risk as an asset. Risk management prior to program execution can help avoid untenable risk management situations during execution. Next year's focus will be on applying risk management during these early phases of the program life cycle. Two of our business ventures are already doing this. They are on hold because of changes in the market and they use risk management to manage the risks of restarting the venture and re-entering the market.

Less Micromanagement. Risk management has been a source of empowerment for our program teams. An initial fear of those presenting risk information at program reviews was that providing detail opened them to micromanagement by senior management. We have found the opposite to be true. Some of highest risk programs exhibit the best functional behavior. They train the entire program team and practice risk management as a team activity. They discuss their risks using the most detail, sometimes as much as two or three slides per risk. After of one such program review, a senior manager remarked, "I can *see you understand your program very well and that you* are making *decisions as well or better than I could in your situation. I don't need to worry about this program. It is very well* managed".

Teams have done significantly better at practicing risk management than individual team leaders. No one has all the necessary knowledge or experience. A risk appears different to different team members depending their perspective (roles, motivations, incentives). For these reasons, three programs trained and involved virtually everyone on the program. The quote above was directed to one of these program teams. Another senior manager said: "I'm more *accepting of surprises from programs doing a good job of risk* management. *I know they're trying to work the risks but stuff happens."*

An Enabling Technology. To develop software people rely on editors, compilers and analyzers. No one would think of conducting a large software development without them. They are the enabling technologies for software development. But what are the enabling technologies for decision making? Those programs that have been practicing risk management the longest view this technology as something they wouldn't do without. Program teams use risk templates to communicate risks with their customers, with other programs and with support organizations. The standalone nature of the detailed information provided in the risk templates enhances their use outside reviews. When risk information has been shared with customers the results are generally positive.

SUMMARY. Our experience has shown that functional behavior is the key element in achieving effective risk management. Implementing and honing a repeatable process and making available additional sources of knowledge, while necessary, cannot alone change behavior. However, a focus on functional behavior can leverage these other two elements. Functional behavior is not simply the converse of dysfunctional behavior. Although in general dysfunctional behaviors must be eliminated, specific new behaviors must be encouraged. These include both what is discussed and how it is discussed. Regular observation, evaluation and coaching of specific risk management behaviors can speed organizational change.

ACKNOWLEDGEMENTS. We would like to thank the program teams of Rockwell Collins Air Transport Division and specifically their senior management, Ron Coffin, Jerry Gaspar and Steve Piller, for their continued support. We also give special thanks to Dr. Robert N. Charette for his many years of advice and support.

REFERENCES

[1] D. Barry, 'A New Rack Record', *Lafayette Journal & Courier,* June 26, 1995 (column, pictures and videos of the event can be found at: *http: / Ighg.ecn.purdue.edu /)*

[2] R. Charette, *Software Engineering Risk Analysis* and Management, McGraw Hill, 1989, pp. 49-57

[3] C. Marshall, L. Prusak and D. Shpilberg, "Financial Risk and the Need for Superior Knowledge Management", California *Management Review,* Vol. 38, No. 3, Spring 1996, pp. 77-101

[4] R. Kirkpatrick, Risk *Management* Culture (videotape), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1993

[5] R. Charette, *Motivation for Software Risk* Management (videotape), Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, 1993

[6] A. Gemmer, "Engineering a Culture for Risk Management", *Fourth SEI Conference on Software Risk,* Monterey, CA, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA, Nov. 1995

[7] R. Charette, M. White and K. Adams, "Establishing Risk Management in an Operational Maintenance Organization", paper submitted to *IEEE Software,* May 1997

[8] R. Charette, *Applications Strategies for Risk* Management, McGraw Hill, 1990, pp. 455463

[9] J. Hammond and J. Morrison, *The Stuff Americans Are Made Of,* MacMillan, New York, NY, 1996, pp. 23-33, 181-215

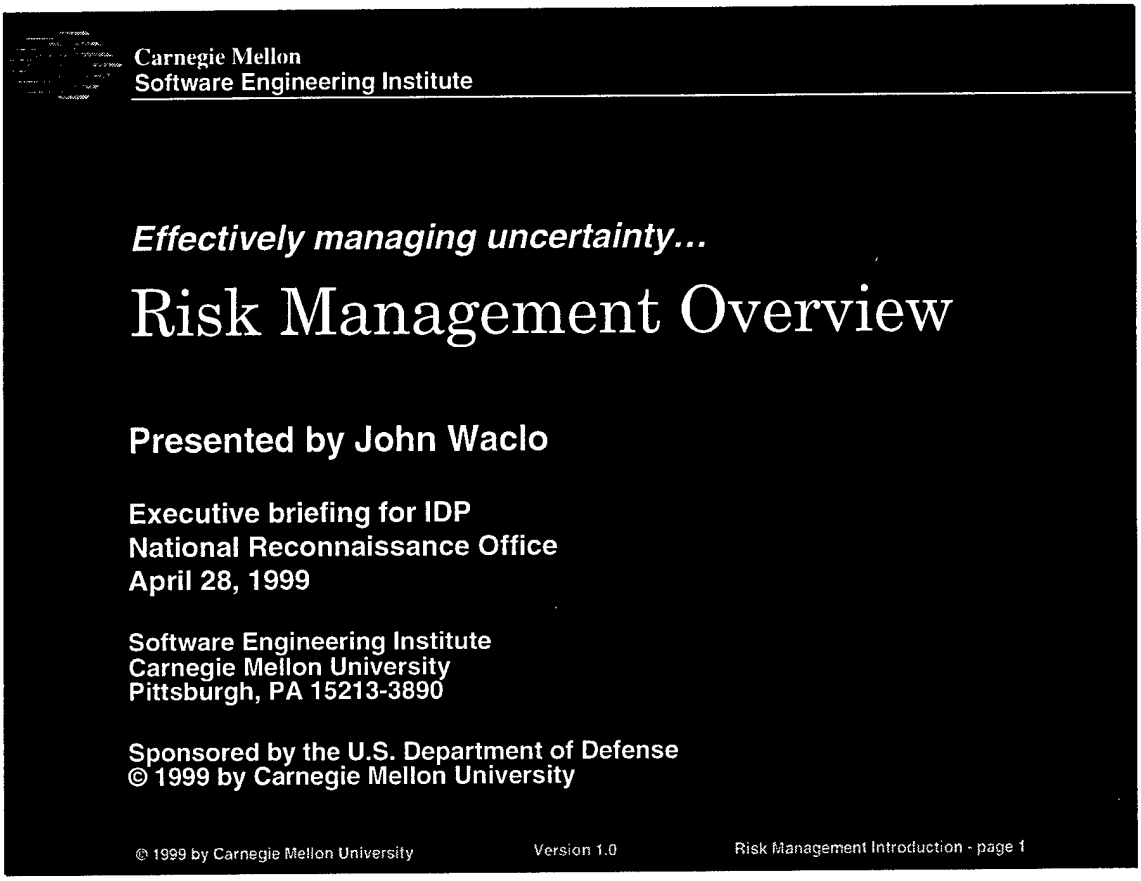
[10] A. Tversky, and D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases", *Science,* Vol. 185, September 1974

[11] *Organizational Learning In* Action (training course), Action Design, Amherst, MA, 1995

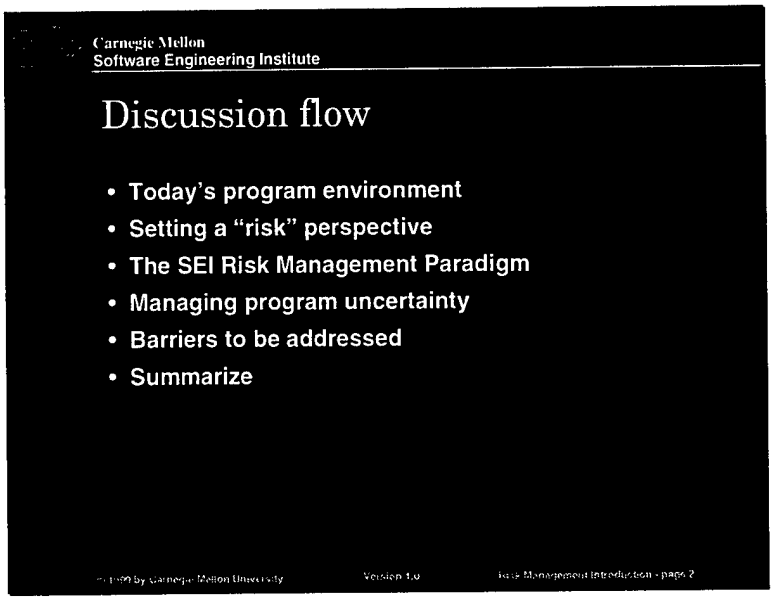
[12] R. Charette, "On Becoming a Risk Entrepreneur", American Programmer, Vol. 8, No. 3, pp.10-15,1995

A.3 Presentation: "Effectively Managing Uncertainty"

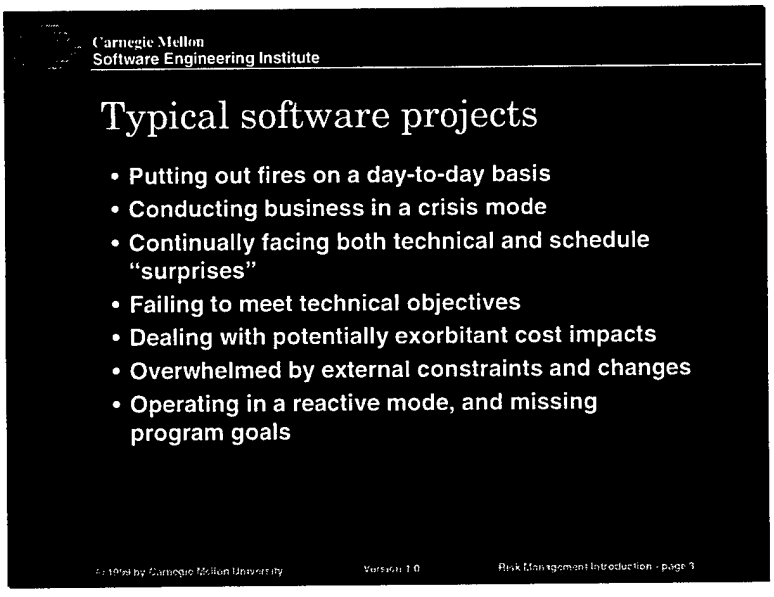
Slide 1



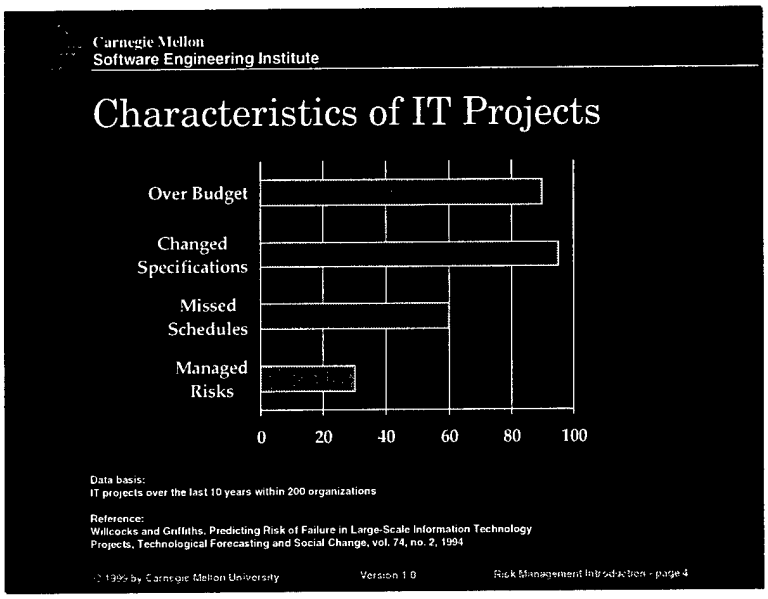
Slide 2



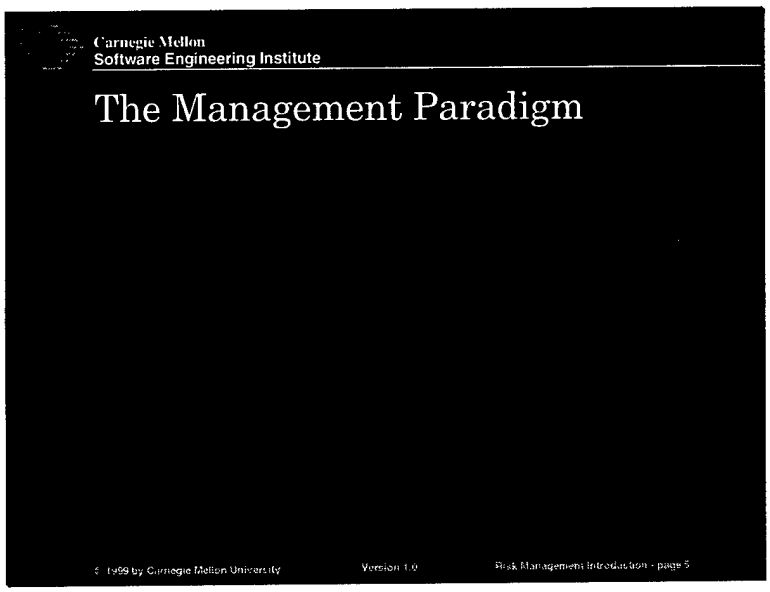
Slide 3



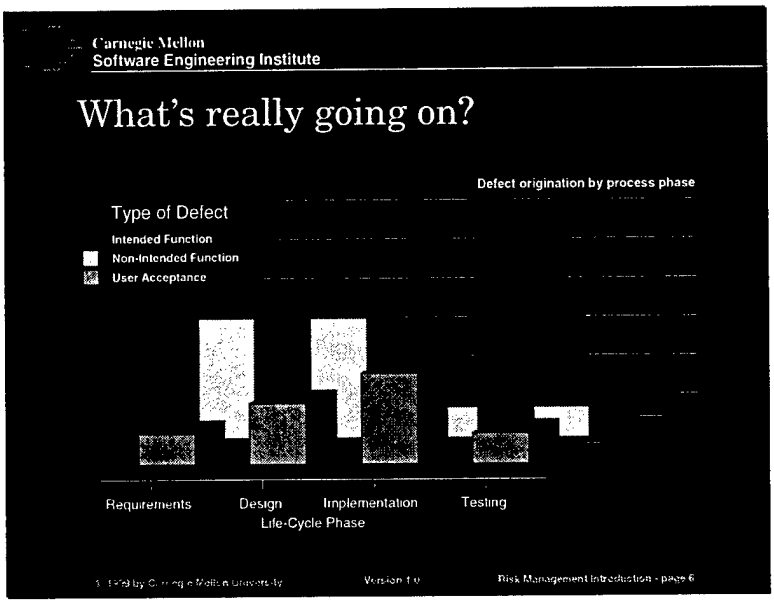
Slide 4

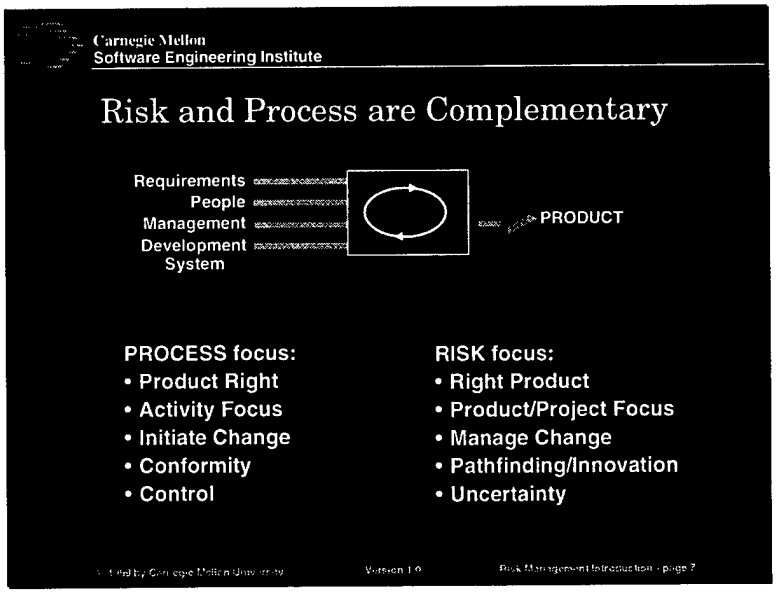


Slide 5



Slide 6


Carnegie Mellon
Software Engineering Institute
What's really going on?
Defect origination by process phase
Type of Defect
Intended Function
Non-Intended Function
User Acceptance
Requirements
Design
Implementation
Testing
Life-Cycle Phase
Version 1.0
Risk Management Introduction - page 6


Carnegie Mellon
Software Engineering Institute
Risk and Process are Complementary
Requirements
People
Management
Development
System
PRODUCT
PROCESS focus:
• Product Right
• Activity Focus
• Initiate Change
• Conformity
• Control
RISK focus:
• Right Product
• Product/Project Focus
• Manage Change
• Pathfinding/Innovation
• Uncertainty
Version 1.0

Slide 8

Carnegie Mellon
Software Engineering Institute

Risk Perspectives

Risks are future events with a probability of occurrence and a potential for loss.

About risks:

- With a timely discovery, risks can be avoided, eliminated, or have their impacts lessened.
- A problem is a risk whose time has come.
- Many of the problems that arise were first known as risks by someone in the project structure.

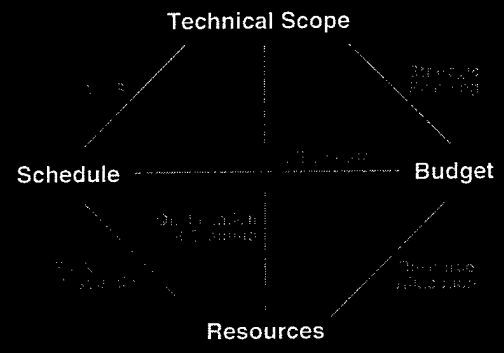
 Version 1.0 Risk Management Introduction - page 8

Slide 9

Carnegie Mellon
Software Engineering Institute

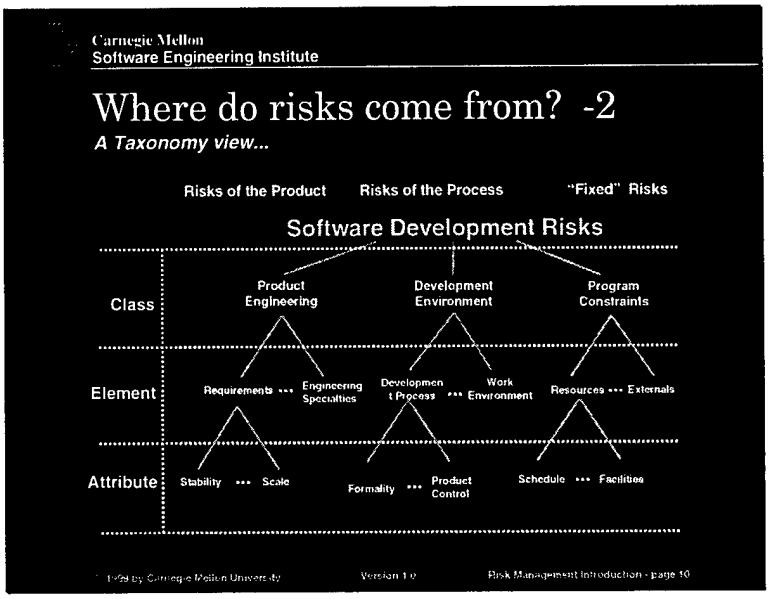
Where do risks come from? -1

A Program view...

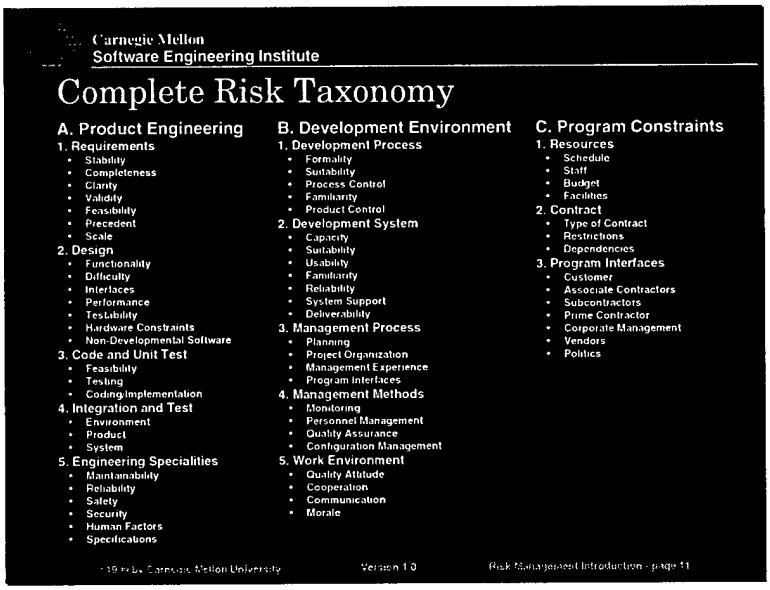


 Version 1.0 Risk Management Introduction - page 9

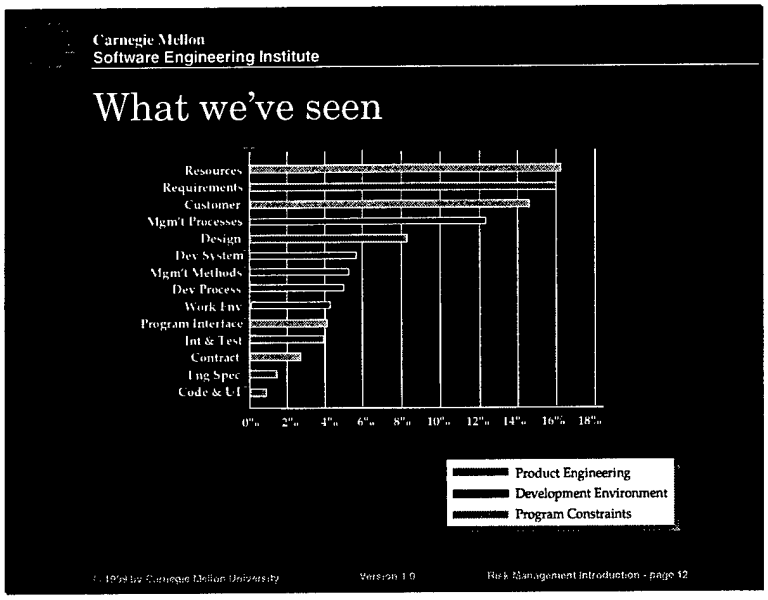
Slide 10



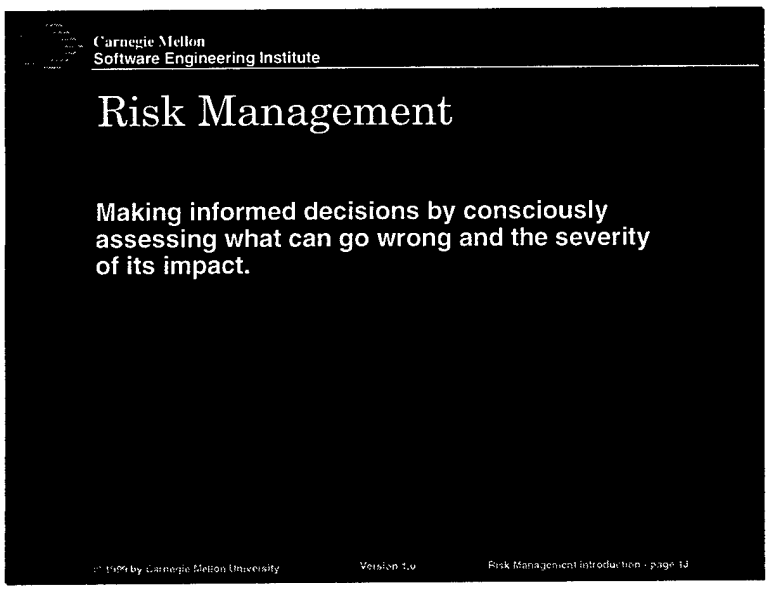
Slide 11



Slide 12



Slide 13



Slide 14

Carnegie Mellon
Software Engineering Institute

Continuous Risk Management

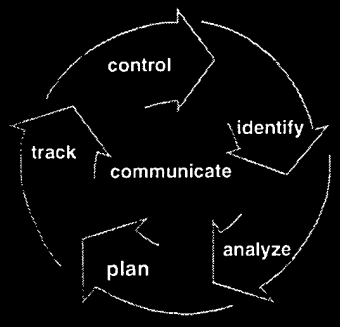
CRM provides a structured and disciplined approach for proactive decision making. Basically, risk management is comprised of three steps:

- Continuously assessing what could go wrong (risks) in a project
- Determining which risks are important to address
- Developing and implementing strategies to deal with important risks

 Version 1.0 Risk Management Introduction - page 14

Carnegie Mellon
Software Engineering Institute

SEI Risk Management Paradigm



 Version 1.0 Risk Management Introduction - page 15

Slide 16

Carnegie Mellon
Software Engineering Institute

Identify characteristics...

Why
- To openly identify risks so they can be managed
- To state risks in a format that can be actively addressed

Goal
- A systematically obtained list of actionable risks

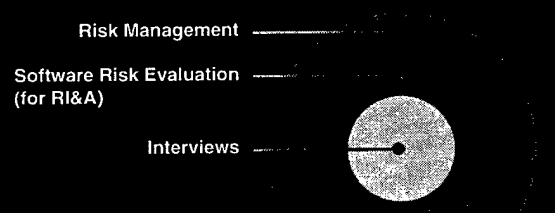
Focus
- To seek multiple individual perspectives
- To seek multiple sources of information

 Version 1.0 Risk Management Introduction - page 16

Slide 17

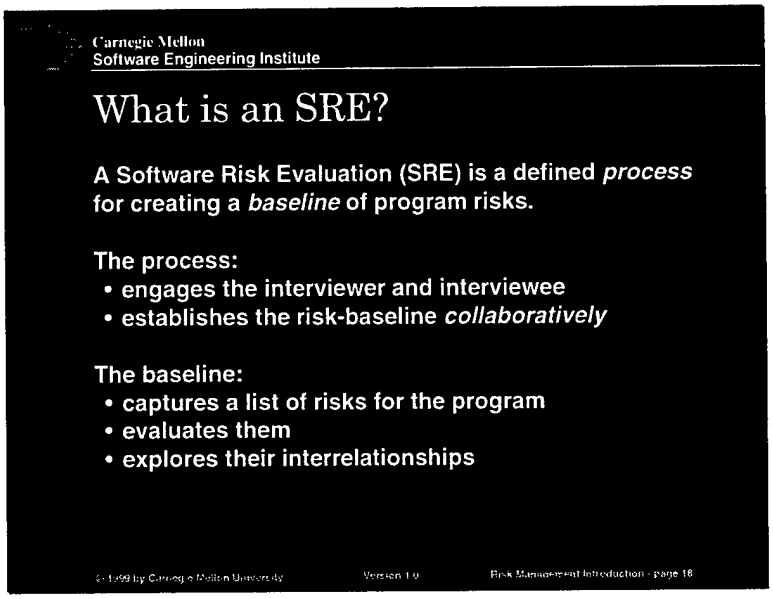
Carnegie Mellon
Software Engineering Institute

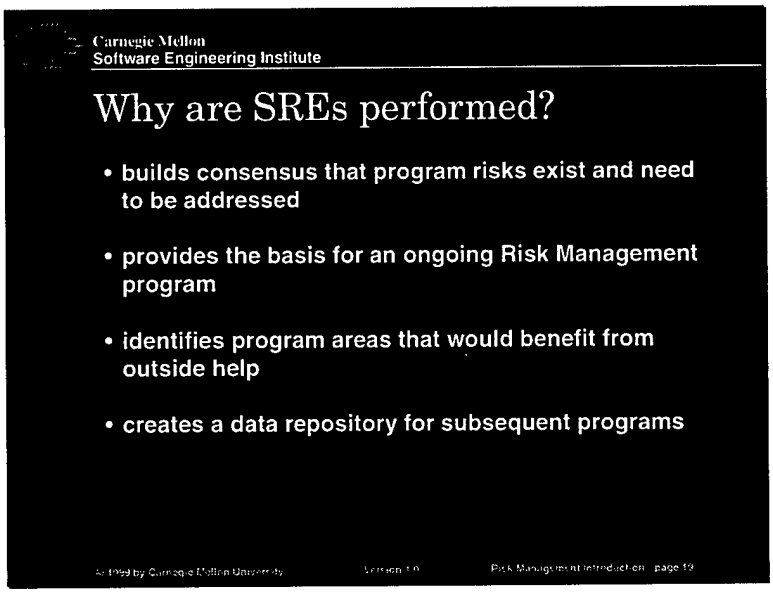
Context for the SEI Software Risk Evaluation (SRE)



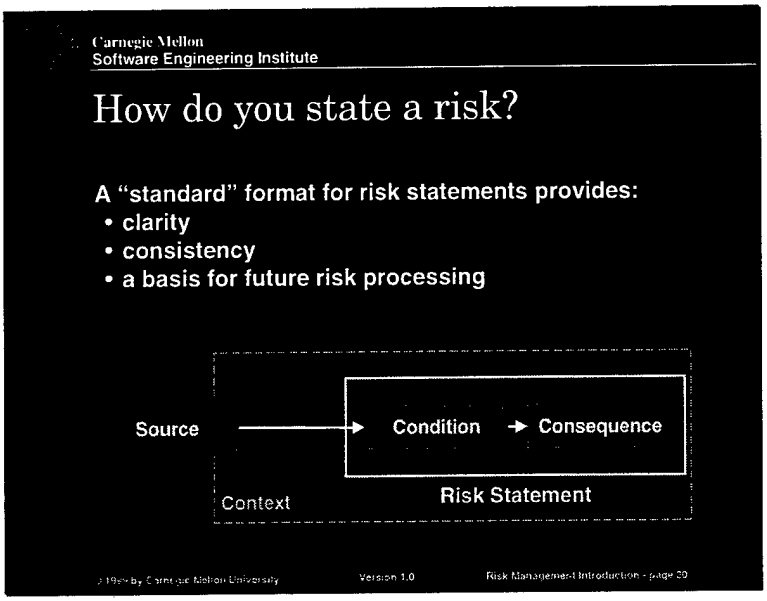
 Version 1.0 Risk Management Introduction - page 17

Slide 18

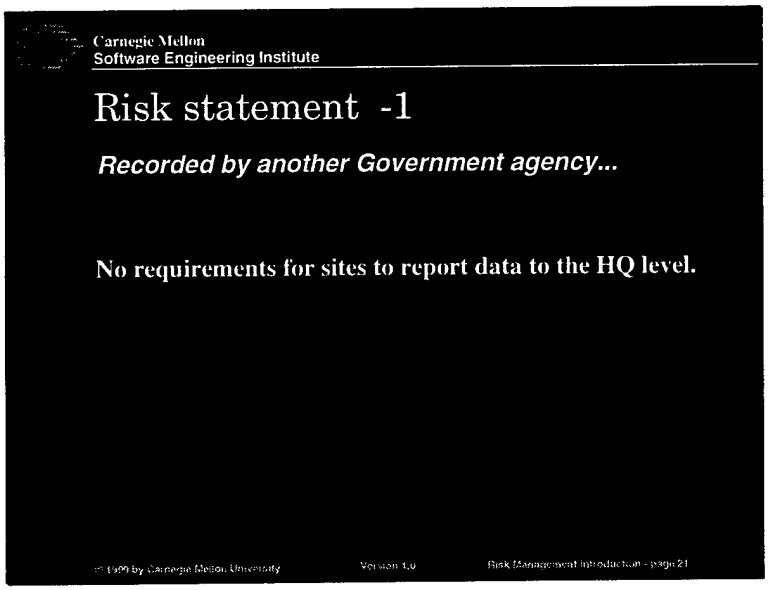

Carnegie Mellon
Software Engineering Institute
What is an SRE?
A Software Risk Evaluation (SRE) is a defined process for creating a baseline of program risks.
The process:
• engages the interviewer and interviewee
• establishes the risk-baseline collaboratively
The baseline:
• captures a list of risks for the program
• evaluates them
• explores their interrelationships
© 1999 by Carnegie Mellon University
Version 1.0
Risk Management Introduction - page 18


Carnegie Mellon
Software Engineering Institute
Why are SREs performed?
• builds consensus that program risks exist and need to be addressed
• provides the basis for an ongoing Risk Management program
• identifies program areas that would benefit from outside help
• creates a data repository for subsequent programs
© 1999 by Carnegie Mellon University
Version 1.0
Risk Management Introduction - page 19

Slide 20



Slide 21



Slide 22

Carnegie Mellon
Software Engineering Institute

Risk statements -2

There has been inadequate schedule discipline (milestones, slippage, monitor progress, good project management) on this project; with no intervention the project will continue to slip & slide.

Lack of executive sponsorship (maybe because of change in the Administration). Consequences are time delays, frustrations, credibility, and morale. [One of the state departments co-sponsoring the project] may pull out of [the project].

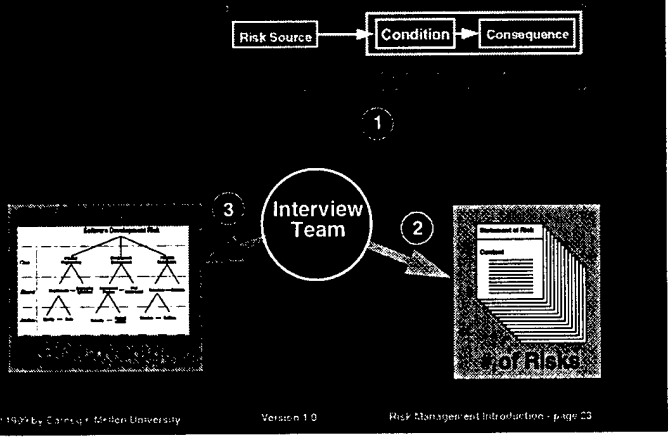
[The project] doesn't have a formal priority for resources; project slippage and waste of resources.

 Version 1.0 Risk Management Introduction - page 22

Slide 23

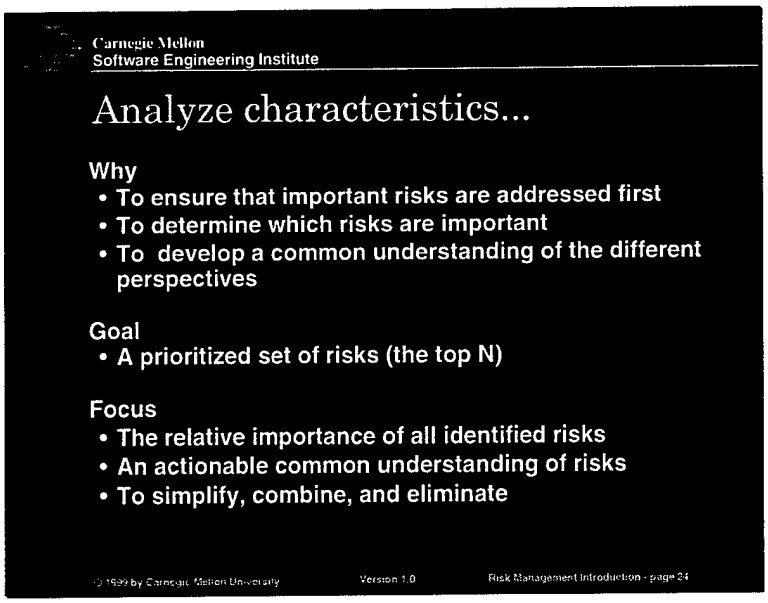
Carnegie Mellon
Software Engineering Institute

Risk interview priorities

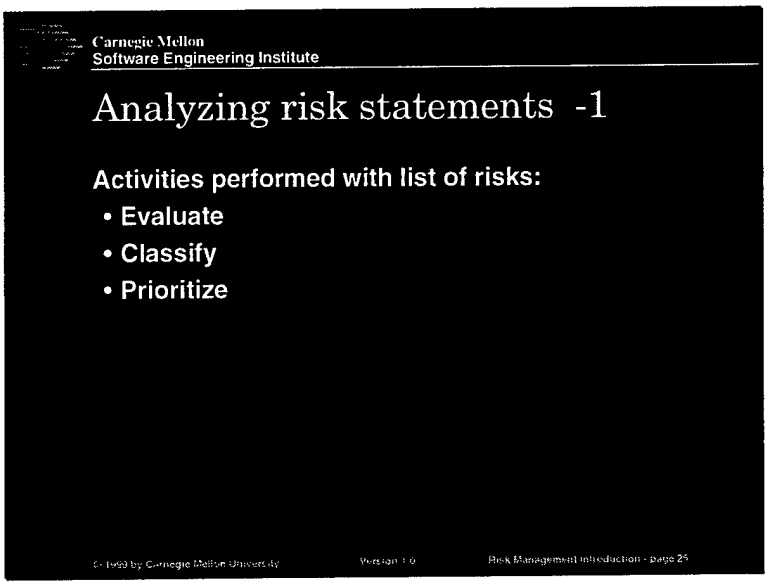


 Version 1.0 Risk Management Introduction - page 23

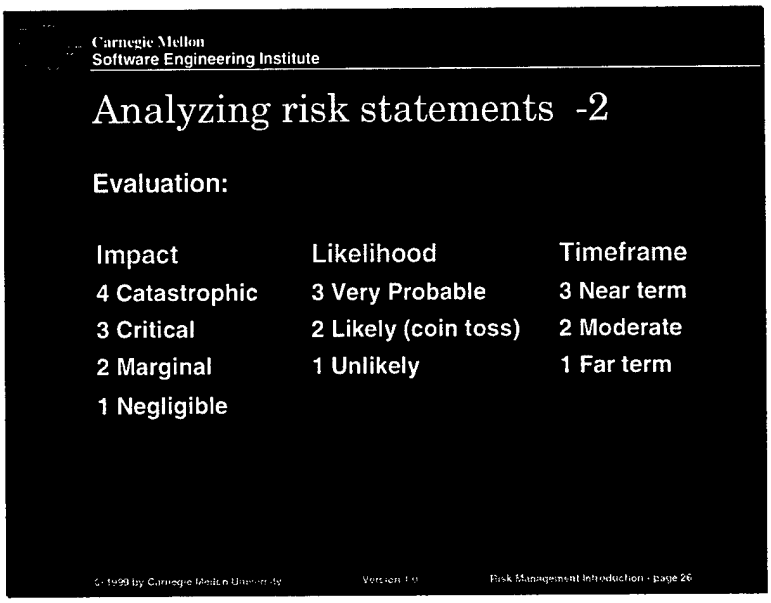
Slide 24

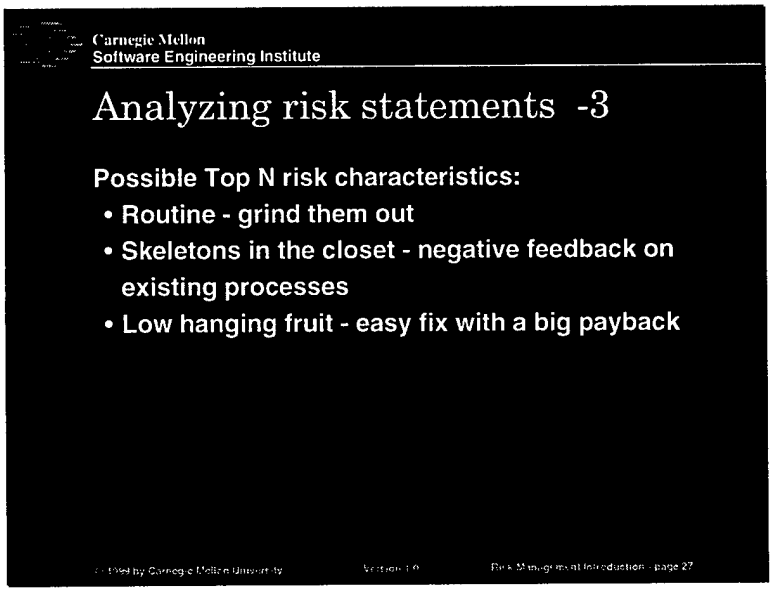


Slide 25

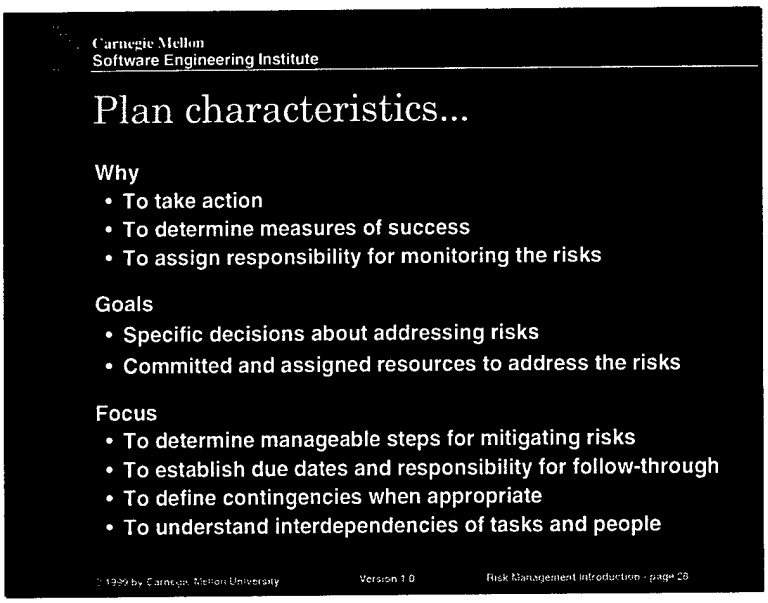


Slide 26

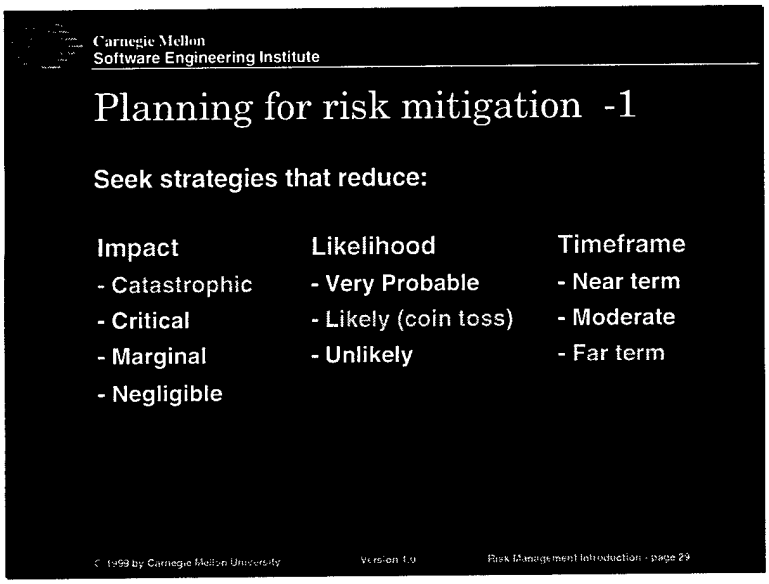

Carnegie Mellon
Software Engineering Institute
Analyzing risk statements -2
Evaluation:
Impact
4 Catastrophic
3 Critical
2 Marginal
1 Negligible
Likelihood
3 Very Probable
2 Likely (coin toss)
1 Unlikely
Timeframe
3 Near term
2 Moderate
1 Far term
Risk Management Introduction - page 26


Carnegie Mellon
Software Engineering Institute
Analyzing risk statements -3
Possible Top N risk characteristics:
• Routine - grind them out
• Skeletons in the closet - negative feedback on existing processes
• Low hanging fruit - easy fix with a big payback

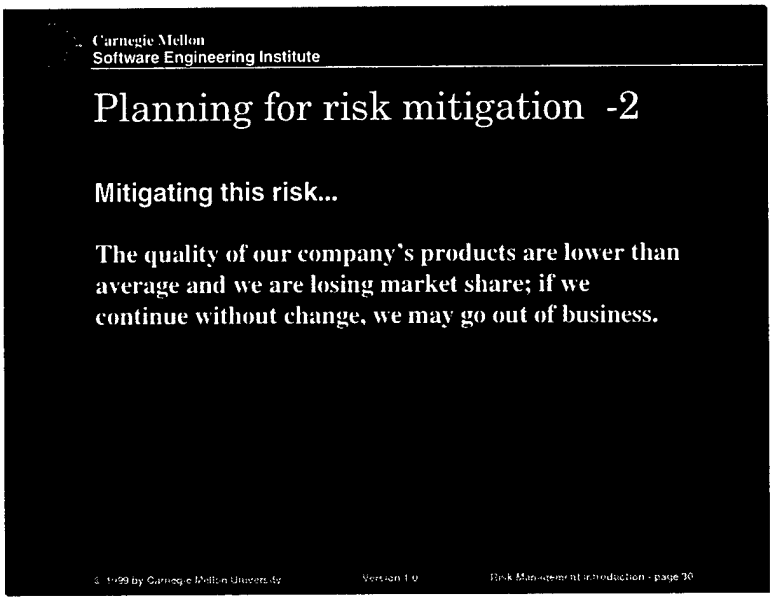
Slide 28



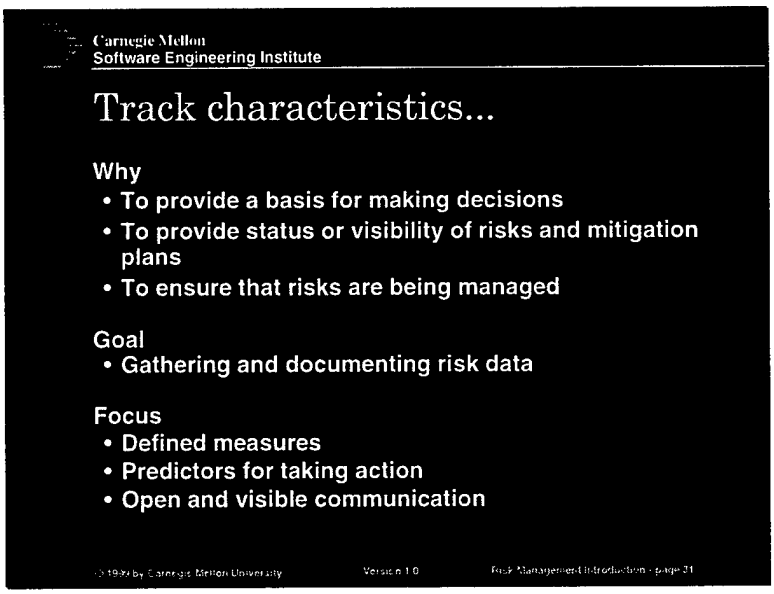
Slide 29



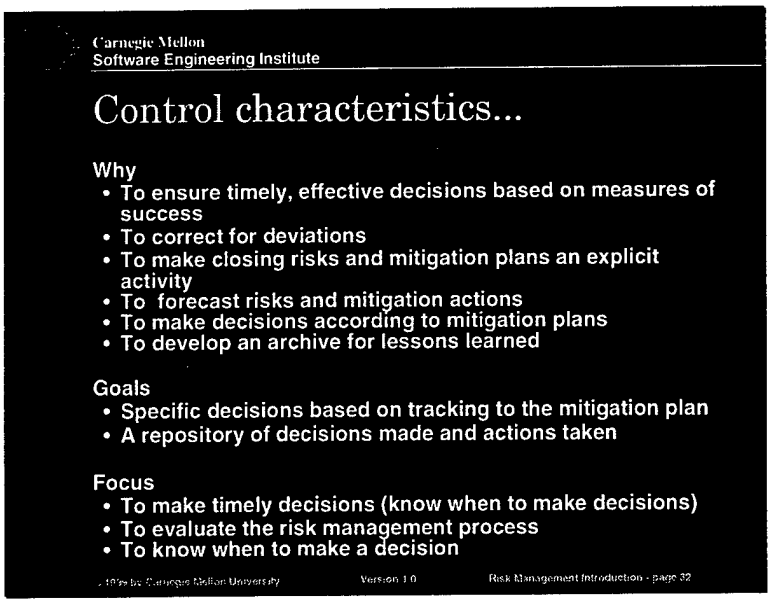
Slide 30



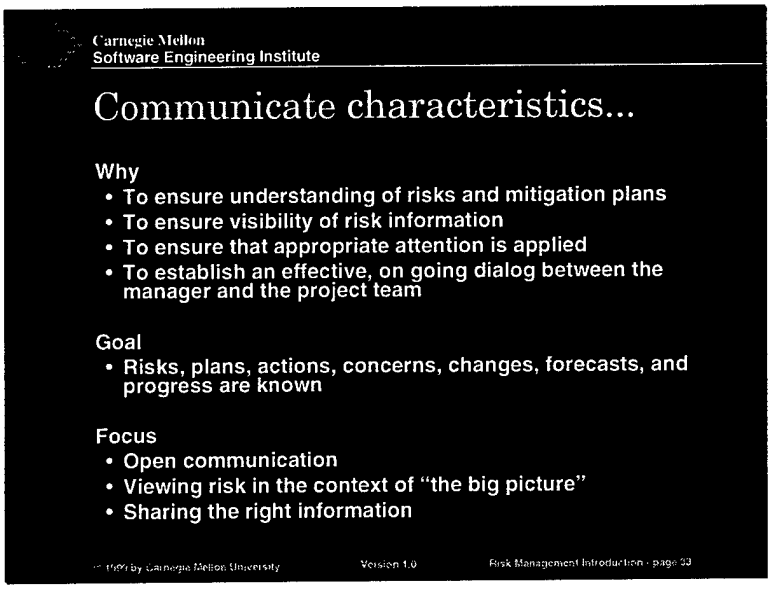
Slide 31



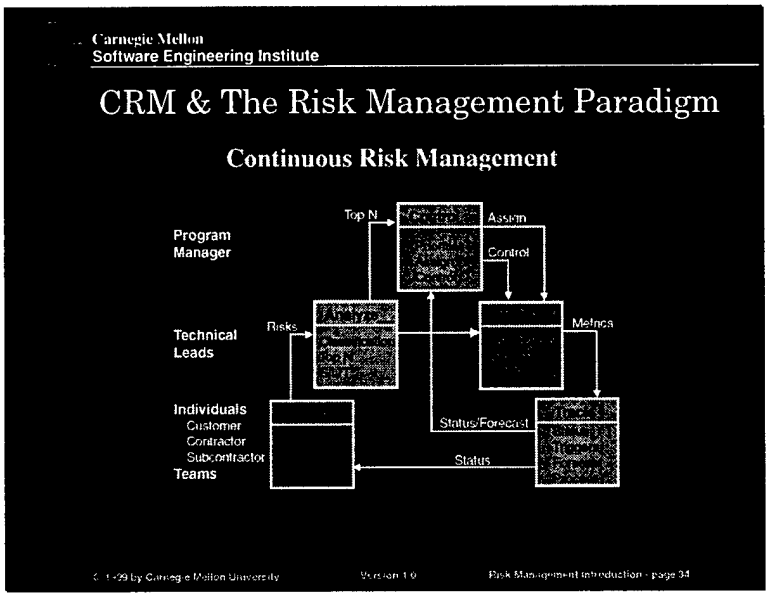
Slide 32



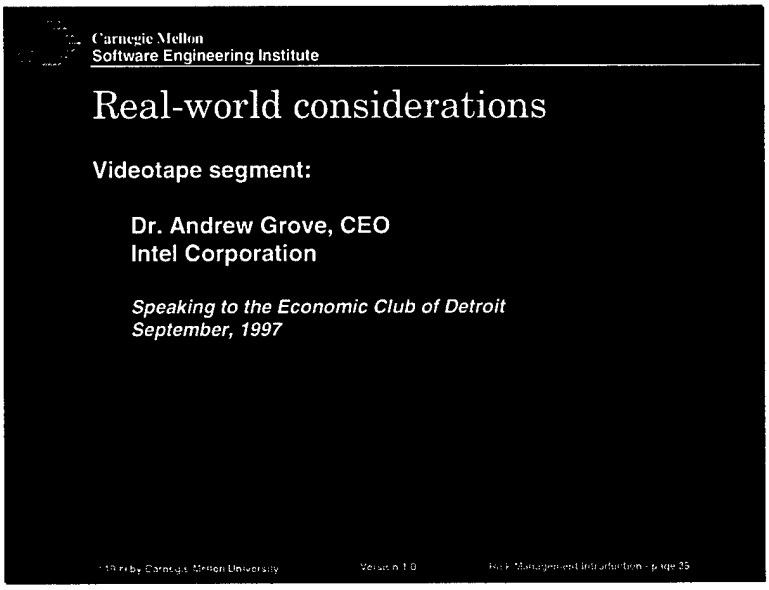
Slide 33



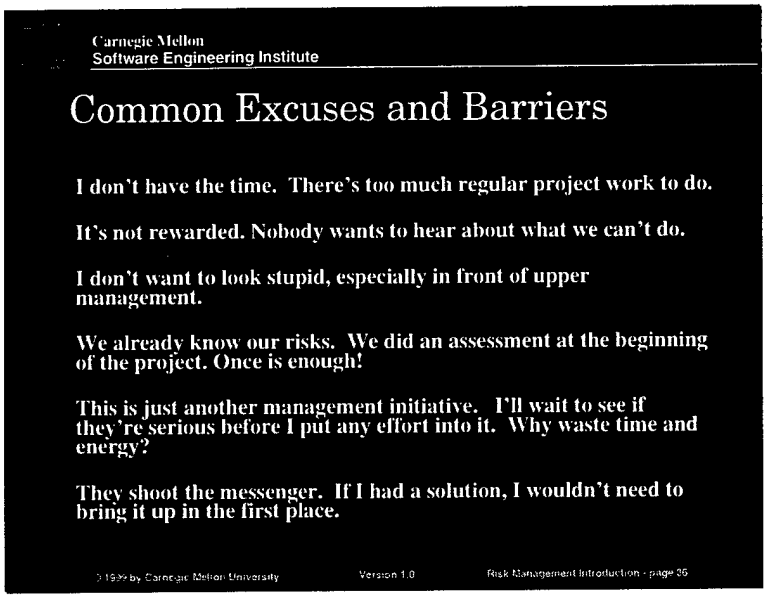
Slide 34



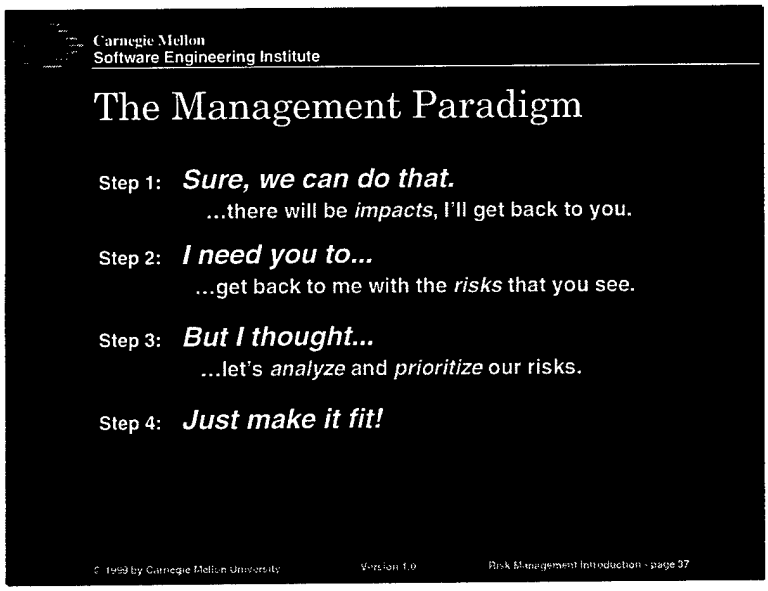
Slide 35



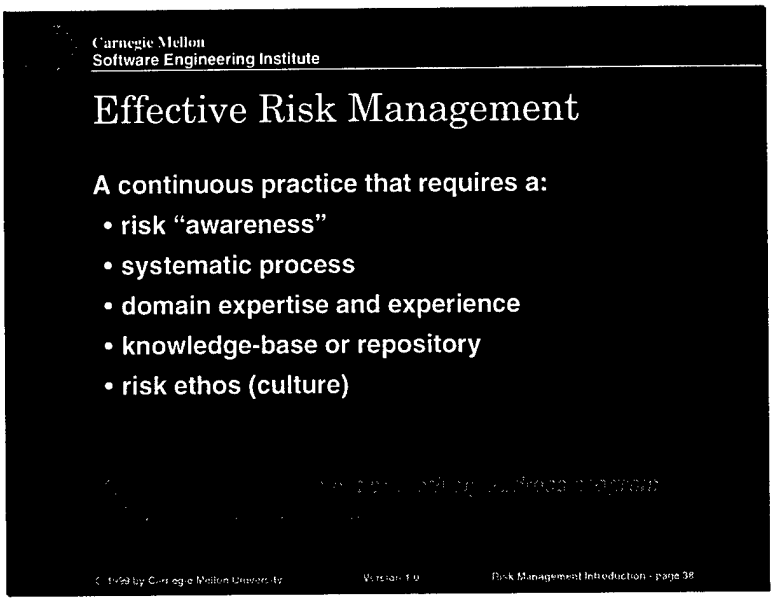
Slide 36



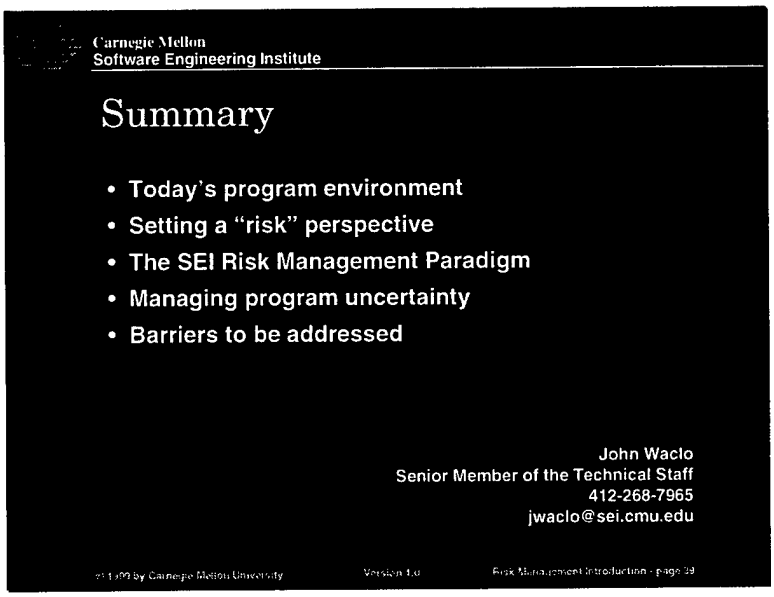
Slide 37



Slide 38



Slide 39



A.4 Sample Team Risk Review Agenda

AGENDA CCD TRR • 13 JANUARY 99 • GAITHERSBURG • 830-1200
Facilitator: Jo Lee Loveland Link • Scribe: John Seewagen • Tmekeeper: JobnSchiphorst

Time	Item Outcome	Lead
830-900	1. TRR Roundtable: Team members on board, pertinent information shared • Identify concerns, opportunities, linkages • RMT Tool update • Seg 4 metrics update • Seg 4 metrics update • Other items of common interest	JLLL, All
900-915	2. Report on TRR Actions Discussion, team decision/recommendations as appropriate	J. Seewagen
915-1000	3. Review Status of all Shared Previously-identified risks are monitored; Customer/Supplier Risk status is noted and updated	Gus, Kevin, All
1000-1015	4. Break Participants refreshed	All
1015-1045	5. New Program Risk New risk described, discussed; decision made whether to add to master list; if added, assigned for attribute definition and mitigation planning	D. Peavy
1045-1115	6. Additional New Seg 4/System-level Risks Identified and Discussed New risks identified, decided whether to be added to master risk list/leveraged for Gus to address at ESRT; assignments made as appropriate	JLLL, All
1115-1145	7. Review Assigned Actions/Select Next TRR Date Actions checked, TRR date set	JLLL, All
1145-1200	8. Success Stories, Lessons Learned; "Reports from the field" noted; process reviewed; potential enhancements noted TRR Meeting Evaluation & Adjourn	JLLL, All

A.5 Culture and Sponsorship

What are the Key Essentials for Managers to Create a Risk Management Culture? The First Line of Defense

The operating assumptions and ability to support business goals are always manifested first in what managers demonstrate to be true, not in what is written down or inferred from designs or procedures.

Most of all, in any change of culture, managers need to show sponsorship—and become sponsors who *communicate.* "Leaders do not have a choice about *whether* to communicate," says organizational culture practitioner Edgar Shein, "they have a choice only how much to plan and direct what they communicate. Sponsors 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 in organizations hear and believe; it is the entire range of messages sent through behaviors and their consequences, organizational mechanisms, and events that have impact.

To communicate effectively, especially in organizations undergoing a great deal of change from within or without, successful sponsors incorporate Risk Management in their vision, communicate the alignment between the vision and how Risk Management supports achieving that vision, and provide reinforcement mechanisms to enforce the integration of effective Risk Management practices into everyday business operations. The following are ways in which this can be done.

1. **Successful sponsors pay attention to, measure, and control desired risk practices, activities, and behaviors.**
- "What gets measured get performed": ask about it; integrate it into the "way we do business around here" in plans, meetings, reviews, reports.
- *Consistency* is more important than *intensity;* that is, consistency sends clear signals, vs. one-time major message: make sure that executive oversight includes regular insight into risk practices throughout the organization.

2. **Successful sponsors react to critical incidents and organizational crises in ways that reinforce the core messages.**
- Open communication avoids "killing the messenger" when raising issues that need attention.

- Hold to planned strategies and improvement processes: even—perhaps *especially*—in crisis, reinforce that there is a new "standard operating procedure" to continue forecasting risks even while addressing current problems ("risks whose time has come").
- While organizational heroes are given their due, they are not held up as models for permanent organizational functioning: by contrast, those who quietly perform high-quality processes and improvement approaches are acknowledged as preventing crises.

3. **Successful sponsors intentionally provide role modeling, coaching, and teaching.**

- Not only by "walking around," but through serving as role models, sponsors provide reinforcement that values and recognizes ideas regardless of organizational level.
- By example, sponsors show how to create conditions for success that align with the organization's business goals.
- Sponsors can take a leadership role through a process of *mutual accountability*—joint responsibility in a partnership between senior management, program managers, and technical practitioners for derailments, modeling accountability while holding others accountable as well, and working together to generate better outcomes.

4. **Successful sponsors reward and recognize publicly activities and job performance that support the goals sought; making clear how rewarded behaviors are determined.**

- In addition to rewarding good risk managers, sponsors provide necessary resources *when they are needed* wherever possible, and reward constructive problem-solving where budgetary and personnel resource constraints are tight.
- Performance goals and reviews specifically include items that recognize and hold people accountable for active support of Risk Management practices and mechanisms to achieve these practices.

5. **Successful sponsors develop and apply specific criteria used to recruit, select, promote, retire, and exclude on the basis of the organization's business goals and priorities.**

- Nordstrom's hires based on customer attitudes; Honeywell and Microsoft hire based on readiness to perform on teams; Risk Management needs to be on the criteria list of selection of those entrusted with responsible positions.
- Managers who serve as role models and coaches for Risk Management are supported and recognized themselves.

A word of caution: These are successful only if they are consistent with "first line of defense" sponsorship. If there are mixed messages, the "second line" mechanisms will create internal conflict and widespread skepticism. But if consistent with sponsorship, these are powerful supports to build a culture focused on best Risk Management practices and business goals.

1. **Organizational design and infrastructure: the way work gets done reflects business goals as well as support for business goals.**

   Is the organization trying to break down stovepipes?—Create workable cross-system linkages, formalized and influential, using Risk Management practices to open up communication. Is the organization building system-wide processes?—Create mechanisms that enhance negotiations across projects to assure cohesive, coherent efforts. Is the goal to increase organizational strength and readiness? Either consolidation or decentralization may be appropriate—but in either case, create an organization that is responsive within and without.

2. **Organizational infrastructure, systems, procedures.**

   These can serve to increase stability, enhance credibility, and reduce uncertainty about desired goals, practices, and processes. Risk management efforts, Process action teams, software engineering process groups, business reinvention teams—all provide infrastructure to ensure forums for action. Daily, weekly, monthly, and quarterly reviews and reports can reinforce "paying attention" by sponsors, and provide information with which to heighten accountability.

3. **Organization of physical space.**

   Being thoughtful about space organization can pay dividends. Beware of the ready-made solutions: unorthodox use of space (and time in a given space) can help create different outcomes from past derailments and stagnation. Think through the actual mechanisms involved in a culture that support surfacing risk identification, and optimum involvement in developing risk mitigation strategies. In planning projects, for example, consider business goals while assigning space—a business goal for more inter-organizational cooperative efforts does not automatically mean physical proximity, but rather acknowledgement of the value of integrating different perspectives, which could mean cross-placement of project staff. In meetings, expedite discussion

through experimental use of group configurations. Also, don't overlook the value of space as potential reward for desired behaviors.

4. **Telling the organizational history: stories about important events can reinforce the message.**

   An organization's history has profound impact on its future. However, this is one area where "message management" is difficult and must be carefully handled. However, sponsors may provide inspirational stories themselves, and certainly, being aware of and drawing on the organization's stories is valuable in building a widespread awareness of "where we've been and where we're going." For example, "hero stories" in software organizations often focus on the impossible that was achieved through creative workarounds and long nights—this story could be recast to highlight risk prevention—the "what could have happened" stories creating a new kind of hero.

5. **Formal statements of organizational philosophy, creeds, team charters, and other agreements.**

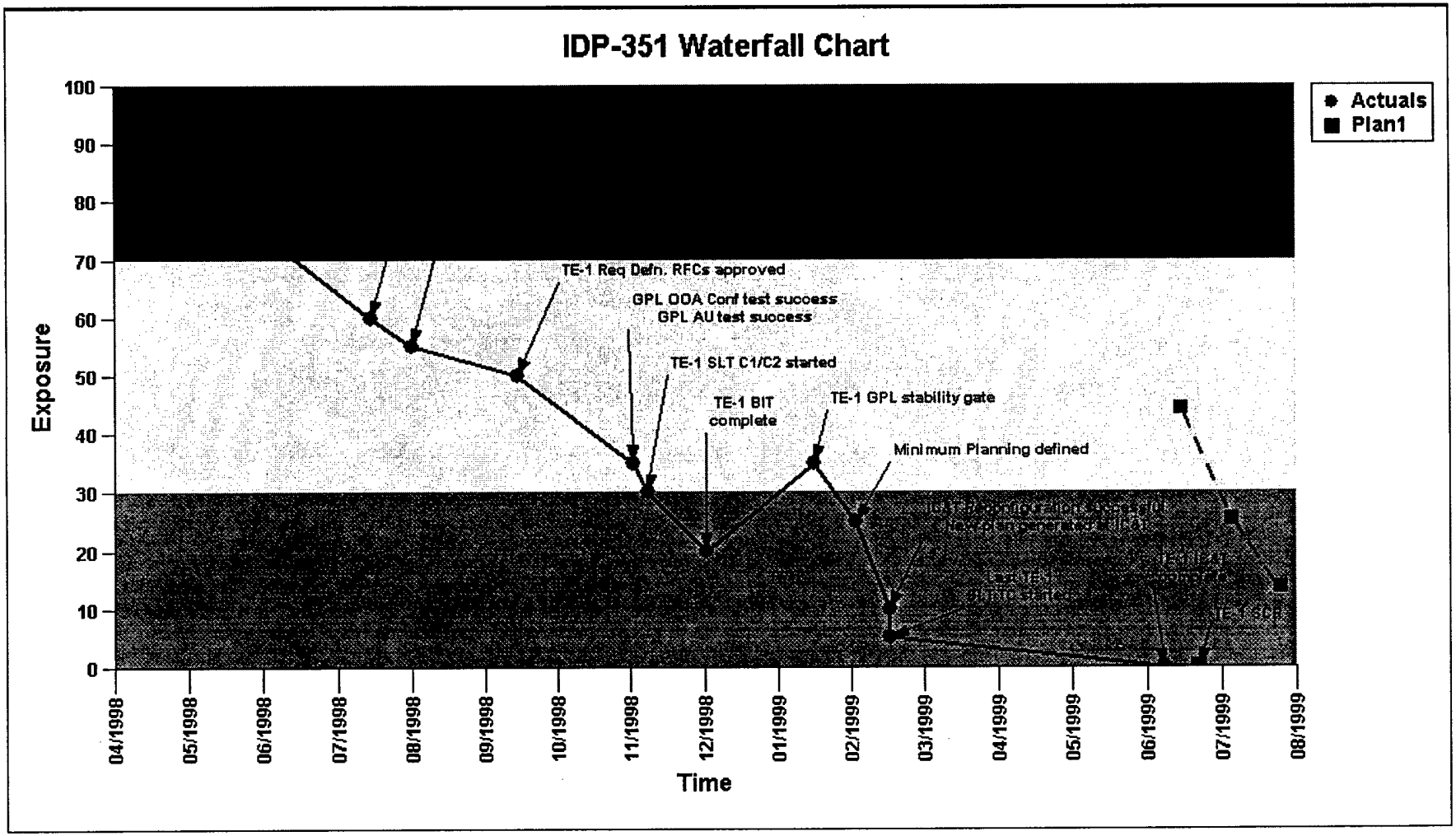
   While the risk is that these documents may not reflect reality, they can—if honestly developed—be powerful tools to build cohesion and integrated focus on Risk Management in an organization. Increasingly, leaders seek input from across organizations for creating statements of vision and mission; teams build their own charters. Document templates that include Risk Management as part of doing business can reinforce good practice.

Adapted by Jo Lee Loveland Link from several sources, primarily from Edgar H. Shein, Organization Culture and Leadership, Jossey-Bass, 1988.

A.6 Waterfall Chart

The waterfall chart provides a graphical view of the status of the risk. The following features are provided:

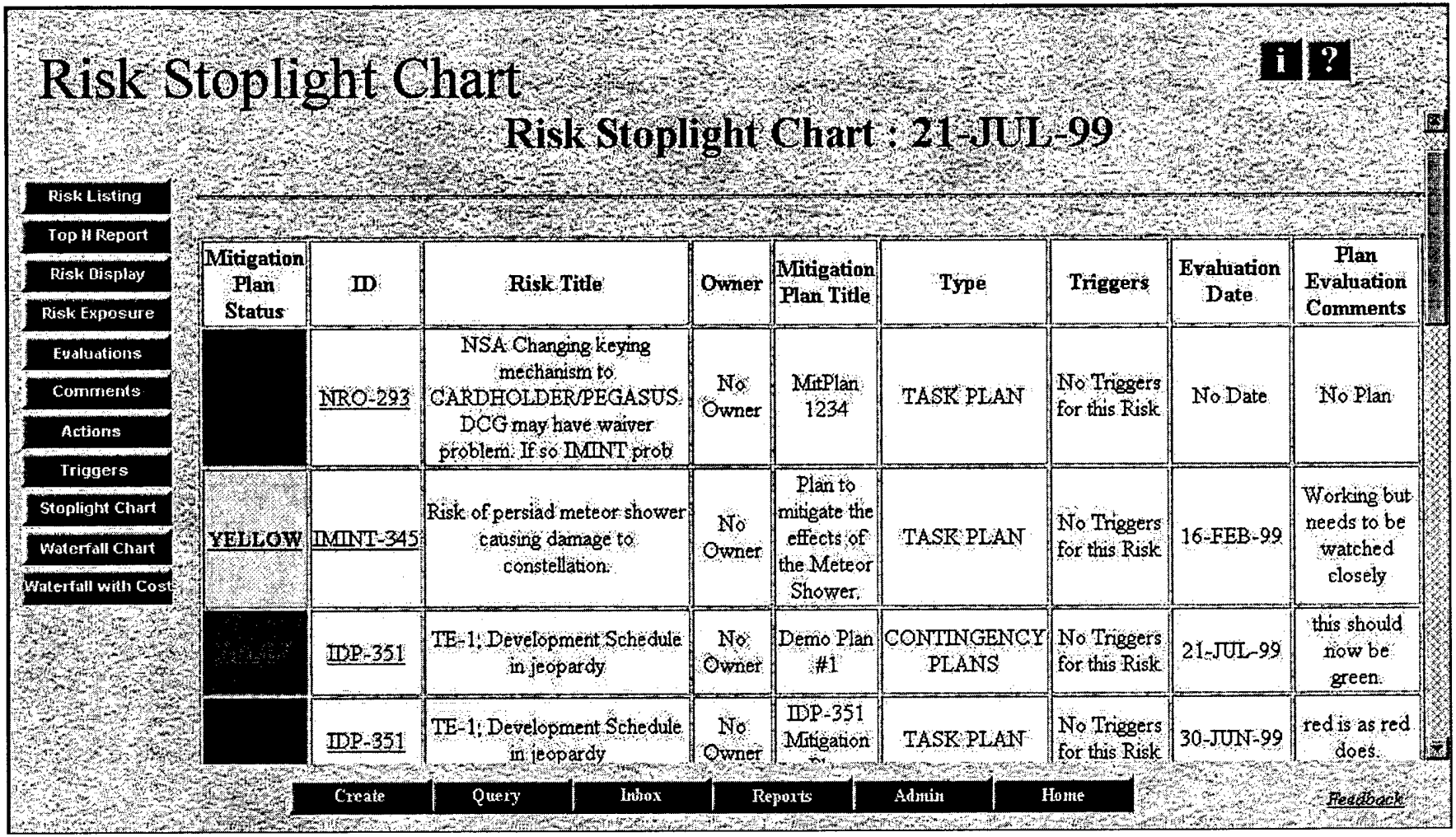
- The X axis displays the relative risk exposure entered in the Risk Management Tool on a particular date (Y axis).
- Previously derived exposures are plotted and connected via a solid line to present a trend view of risk status over time.
- Forecasts of risk exposures are entered in the risk view screen using the same screen format as the evaluation entry screen. The derived relative exposure for these forecasts are depicted as a dashed line over the prescribed timeline. A forecast is a prediction of where a particular mitigation strategy plan will buy down risk exposure on a designated date.
- The charts can by annotated with chart notes.
- Exposure forecasts can be managed from the chart.
- Links are provided to return users to related areas in the application.


IDP-351 Waterfall Chart
Actuals
Plan1
Exposure
100
90
80
70
60
50
40
30
20
10
0
TE-1 Req Defn. RFCs approved
GPL OOA Conf test success
GPL AU test success
TE-1 SLT C1/C2 started
TE-1 BIT complete
TE-1 GPL stability gate
Minimum Planning defined
04/1998
05/1998
06/1998
07/1998
08/1998
09/1998
10/1998
11/1998
12/1998
01/1999
02/1999
03/1999
04/1999
05/1999
06/1999
07/1999
08/1999
Time

A.7 Risk Stoplight Chart

The Stoplight chart provides a graphical view of the effectiveness of each strategy currently employed to buy down the relative exposure of all risks tracked in an organization. Features of this report are as follows:

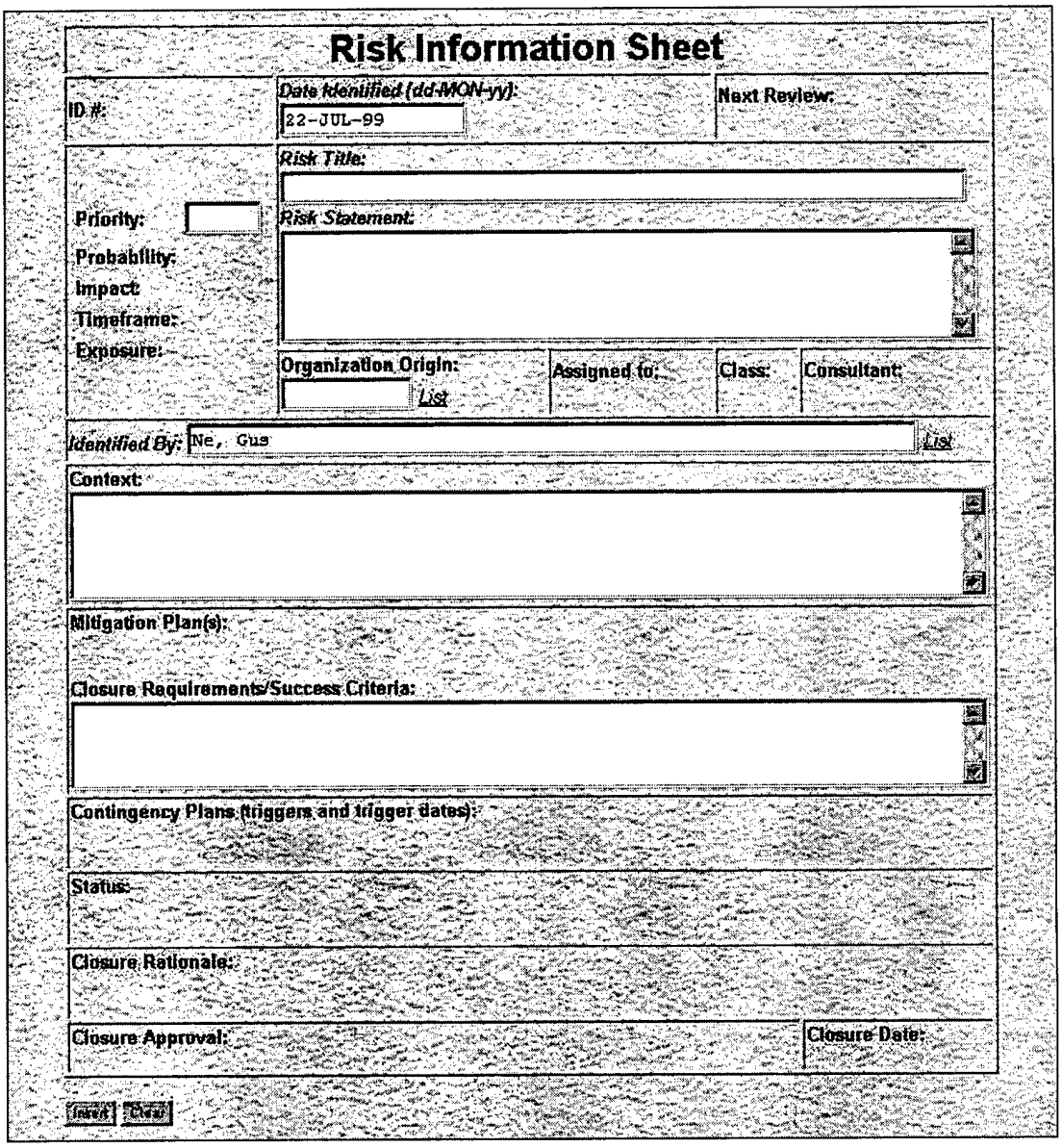
- Color coded cells indicate status.
- Status can be updated from the chart by selecting the color coded cell.
- Detailed Risk Information is provided by selecting the hypertext linked Risk ID.


Risk Stoplight Chart
Risk Stoplight Chart : 21-JUL-99
Risk Listing
Top II Report
Risk Display
Risk Exposure
Evaluations
Comments
Actions
Triggers
Stoplight Chart
Waterfall Chart
Waterfall with Cost
Mitigation Plan Status
ID
Risk Title
Owner
Mitigation Plan Title
Type
Triggers
Evaluation Date
Plan Evaluation Comments
NRO-293
NSA Changing keying mechanism to CARDHOLDER/PEGASUS. DCG may have waiver problem. If so IMINT prob
No Owner
MitPlan 1234
TASK PLAN
No Triggers for this Risk
No Date
No Plan
YELLOW
IMINT-345
Risk of persiad meteor shower causing damage to constellation.
No Owner
Plan to mitigate the effects of the Meteor Shower.
TASK PLAN
No Triggers for this Risk
16-FEB-99
Working but needs to be watched closely
IDP-351
TE-1; Development Schedule in jeopardy
No Owner
Demo Plan #1
CONTINGENCY PLANS
No Triggers for this Risk
21-JUL-99
this should now be green.
IDP-351
TE-1; Development Schedule in jeopardy
No Owner
IDP-351 Mitigation
TASK PLAN
No Triggers for this Risk
30-JUN-99
red is as red does.
Create
Query
Inbox
Reports
Admin
Home
Feedback

A.8 Risk Information Sheet

The risk entry screen has been organized to look and electronically function like the Software Engineering Institute's standard risk entry form, the risk information sheet. The risk information sheet entry screen provides the following fields for initial identification of a risk.

- *date identified*; the date the risk was identified
- *risk title*; the user-defined title of the risk
- *risk statement*; the risk description information
- *priority*; the priority or ranking of the risk against other risks in the system
- *originating organization*; the organization that originated or identified the risk
- *identified by*; the person who identified the risk
- *context*; the context of this risk within the system
- *closure criteria*; the criteria required to close the risk


Risk Information Sheet
ID #:
Date Identified (dd-MON-yy):
22-JUL-99
Next Review:
Risk Title:
Priority:
Risk Statement:
Probability:
Impact:
Timeframe:
Exposure:
Organization Origin:
List
Assigned to:
Class:
Consultant:
Identified By:
Ne, Gus
List
Context:
Mitigation Plan(s):
Closure Requirements/Success Criteria:
Contingency Plans (triggers and trigger dates):
Status:
Closure Rationale:
Closure Approval:
Closure Date:

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (LEAVE BLANK)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1999	Unlimited TR

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Rollout and Installation of Risk Management at the IMINT Directorate, National Reconnaissance Office	C — F19628-95-C-0003
6. AUTHOR(S)	
Jo Lee Loveland Link, Rick Barbour, Al Krum, August C. Neitzel	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-99-TR-009
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-99-009

11. SUPPLEMENTARY NOTES

12.A DISTRIBUTION/AVAILABILITY STATEMENT	12.B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The NRO Risk Management pilot project, and subsequent rollout and installation, were launched in the Imagery Development Program (IDP) at the Imagery Intelligence (IMINT) Directorate. This was preceded by a Software Acquisition Capability Maturity Model® (SA-CMM®) assessment to determine strengths and gaps in IMINT's capability as an acquisition organization. From the potential SA-CMM improvement areas, IMINT leaders determined that the optimum first initiative would be Acquisition Risk Management. To launch the Risk Management initiative, IMINT leaders identified the Command and Control Division (CCD) in IDP as the pilot initiative. They further decided to conduct Software Risk Evaluations (SREs) with both the government organization and the principal contractor for CCD. The CCD division proceeded to install a dynamic, interactive Risk Management process throughout its program, with a Team Risk Management approach. This approach was leveraged by monthly CCD Team Risk Reviews (TRRs). The TRRs served as regular forums for government and contractors to identify and mitigate joint risks. The IDP director, observing the success of the CCD pilot, called for consistent Risk Management training across the divisions. Concurrently, the IDP director also launched the EIS System Risk Management Team (ESRT) with a mission to identify and address system-level risks. The divisional Risk Management processes (including contractor Risk Management) were combined with system-level Risk Management at the ESRT to develop a comprehensive, consistent Risk Management process that became routinely operational. The central purpose of this report is to provide a knowledge asset repository for the National Reconnaissance Office that can be leveraged in support of further Risk Management efforts.

14. SUBJECT TERMS	15. NUMBER OF PAGES
risk management, acquisition risk management, risk mitigation, knowledge management, National Reconnaissance Office, Software Acquisition, Capability maturity Model, CMM.	190
16. PRICE CODE	

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL