Special Report
CMU/SEI-94-SR-1

An Introduction to Team Risk Management

(Version 1.0)

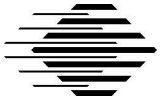
Ronald P. Higuera
David P. Gluch
Audrey J. Dorofee
Richard L. Murphy
Julie A. Walker
Ray C. Williams

May 1994

Special Report
CMU/SEI-94-SR-1
May 1994

An Introduction to Team Risk Management

(Version 1.0)



Ronald P. Higuera
David P. Gluch
Audrey J. Dorofee
Richard L. Murphy
Julie A. Walker
Ray C. Williams

Team Risk Management Project

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

This report was prepared for the

SEI Joint Program Office
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

(signature on file)

Thomas R. Miller, Lt Col, USAF
SEI Joint Program Office

This work is 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.

This document is available through Research Access, Inc., 800 Vinial Street, Pittsburgh, PA 15212.
Phone: 1-800-685-6510. FAX: (412) 321-2994. RAI also maintains a World Wide Web home page. The URL is http://www.rai.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218. Phone: (703) 767-8222 or 1-800 225-3842.]

Table of Contents

List of Figures

List of Tables

An Introduction to Team Risk Management (Version 1.0)

Abstract: (Version 1.0) Team Risk Management defines the organizational structure and operational activities for managing risks throughout all phases of the life-cycle of a software-dependent development program such that all individuals within the organizations, groups, departments, and agencies directly involved in the program are participating team members. Through the adoption of team risk management, the government and contractor are provided with processes, methods, and tools that enable both organizations, individually and jointly, to be increasingly anticipatory in decision-making processes. This report introduces the team risk management approach for managing risks within a software-dependent development program.

1 Introduction

Team risk management provides the government and the contractor with processes, methods, and tools that enable both organizations, individually and jointly, to be increasingly anticipatory in decision-making processes by systematically managing risks in software-dependent development programs. This document describes the processes, methods, and tools that comprise the team risk management approach.

Section 2 provides background for the team risk management approach. The Overview of Team Risk Management, Section 3, outlines risk management and team concepts as they relate to team risk management and introduces the team risk management principles. Section 4, Team Risk Management Processes, initially provides an overview of the major processes of team risk management; subsequent subsections describe each of the continuous processes: routine risk identification and analysis, action planning, tracking, and control as well as a key team activity, the team review. In Section 4.2 the baseline risk assessment is presented and in Section 5 the underlying foundations of team building and communications are discussed. Section 6 provides a summary of the risk management approach and observations from the application of team risk management in real-world programs.

2 Background

As a software-dependent development program unfolds, both the government and the contractor have a vision of the direction and ultimate outcome necessary for the program's success. Unfortunately, all too often the outcome, while shared by both parties, is not as successful as initially envisioned by either party. The unanticipated, the unexpected, the unforeseen often distort the program's progress and ultimate outcome.

To address this situation and to provide government program offices and contractors with approaches for managing program uncertainties (risks) and avoiding their consequences, the Software Engineering Institute's (SEI) Risk Program has developed Team Risk Management. The team risk management approach is founded upon a shared vision for the program that is structured out of the individual views of both the government and contractor and is anchored by open communications. Cooperatively, both the government and contractor work together in team risk management to anticipate and avoid problems by managing program risks.

Specifically, 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 a comprehensive and practical set of processes, methods, and tools that include activities that join the contractor and government together as a "team" to manage program risks. The team characteristics of the approach ensure that the "vital few" risks are aggressively managed and that all risks are cost-effectively managed throughout the life cycle of a software-dependent development program. Team risk management processes, methods, and tools become routine and continuous activities within the program and provide management at all levels with the information required to make informed decisions on issues critical to program success.

Team risk management is a self-sustaining methodology that does not depend upon outside organizations for continued successful operation and process improvement. Consequently, through the adoption of team risk management as an integral part of routine program management, organizations can achieve self-sufficiency in software risk management.

Just as deploying fighters, early warning aircraft, and missile ships does not guarantee that no attack will be made on the Naval Task Force, likewise, team risk management does not guarantee that problems will not occur. It will, though, identify the threats early, help to avoid unforeseen problems, and provide a solid foundation for addressing the problems that do arise.

Team risk management is built upon the work and experience of a diverse group of industrial, government, academic, and military technical and management professionals and is a pragmatic implementation of the principles of effective risk management for software-dependent development programs. Through collaborative research, development, and testing between the SEI and its government and industry clients, the SEI is continuing to improve and test existing products and to develop additional team risk management products to meet client needs.

3 Overview of Team Risk Management

Team risk management defines the organizational structure and operational activities for collectively managing risks throughout all phases of the life cycle of a software-dependent development program such that all individuals within the organizations, groups, departments, and agencies directly involved in the program are participating team members. Team risk management practices bring together individuals within an organization and between organizations to form working teams [Higuera 93].

The team risk management approach is built upon the nine principles summarized in Table 1. These principles combine the SEI risk management paradigm (see Figure 3-1 [SEI 92]) and the concepts of cooperative teams to form the foundation for a comprehensive set of processes, methods, and tools for managing risks in software-dependent development programs.

Principle	Effective risk management requires:
1. Shared product vision	a shared vision for success based upon commonality of purpose, shared ownership, and collective commitment.
2. Forward-looking search for uncertainties	thinking toward tomorrow, anticipating potential outcomes, identifying uncertainties, and managing program resources and activities while recognizing these uncertainties.
3. Open communications	a free flow of information at and between all program levels through formal, informal, and impromptu communication and consensus-based processes.
4. Value of Individual perception	the individual voice which can bring unique knowledge and insight to the identification and management of risk.
5. Systems perspective	that software development be viewed within the larger systems-level definition, design, and development.
6. Integration into program management	that risk management be an integral and vital part of program management.
7. Proactive strategies	proactive strategies that involve planning and executing program activities based upon anticipating future events.
8. Systematic and adaptable methodology	a systematic approach that is adaptable to the program's infrastructure and culture.
9. Routine and continuous processes	a continuous vigilance characterized by routine risk identification and management activities throughout all phases of the life cycle of the program.

Table 1: The Nine Principles of Team Risk Management

Team risk management involves concurrent activities of partner organizations working together to manage program risks. This collective, concurrent activity and the team character of team risk management are represented by the government/contractor team risk management process sphere shown in Figure 3-2, where each partner organization is executing the SEI risk

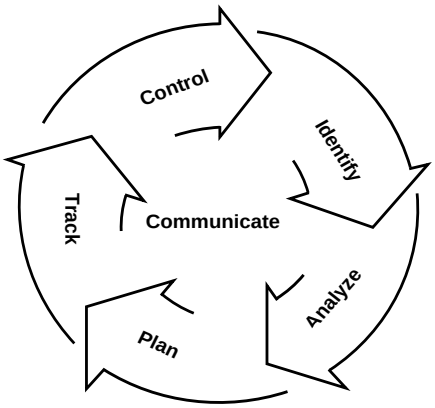


Figure 3-1: The SEI Risk Management Paradigm

paradigm as part of the cooperative team risk management effort. In the case of a software-dependent development program awarded by the government to a primary contractor, there are two partner organizations: the government program office and the contractor.

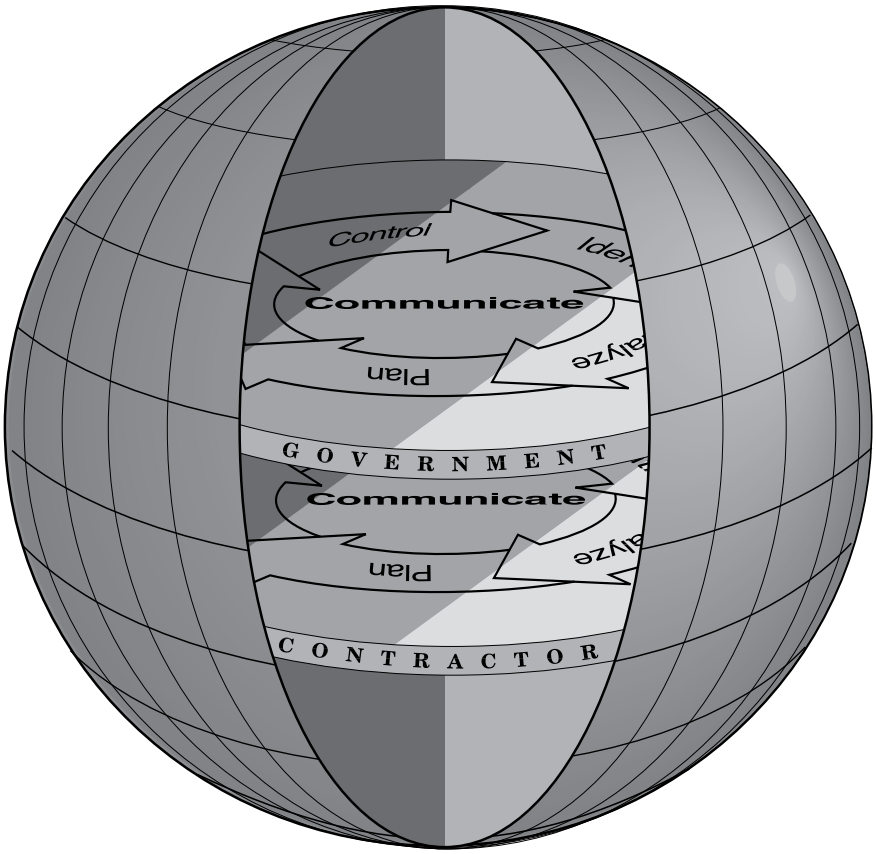


Figure 3-2: The Government-Contractor Team Risk Management Process Sphere

Within team risk management, partner organizations participate in cooperative, inter-organizational “team” activities which are represented by the surface of the team risk management process sphere. Communication, which is represented by the core of the sphere, also interconnects the partners and represents intra-organizational as well as inter-organizational communication processes that are vital to effective team risk management.

While team risk management has been presented in the context of a government /contractor relationship, the concept of team risk management is general. In this broader context, the approach encompasses any customer/supplier relationship such that the team risk management process sphere is divided into the upper hemisphere (customer) and the lower hemisphere (supplier), as shown in Figure 3-3. Each hemisphere may include multiple customer or supplier partner organizations (the term “partner” refers to any individual, group, organization, or department within an organization that is participating in team risk management activities).

Fundamentally, the implementation of team risk management in a government program brings together the government and the contractor in a continuous and collective effort for success, where both are focused on managing program risks. In subsequent sections of this document, the processes, methods, and tools of team risk management as applied to a government software-dependent development program are described.

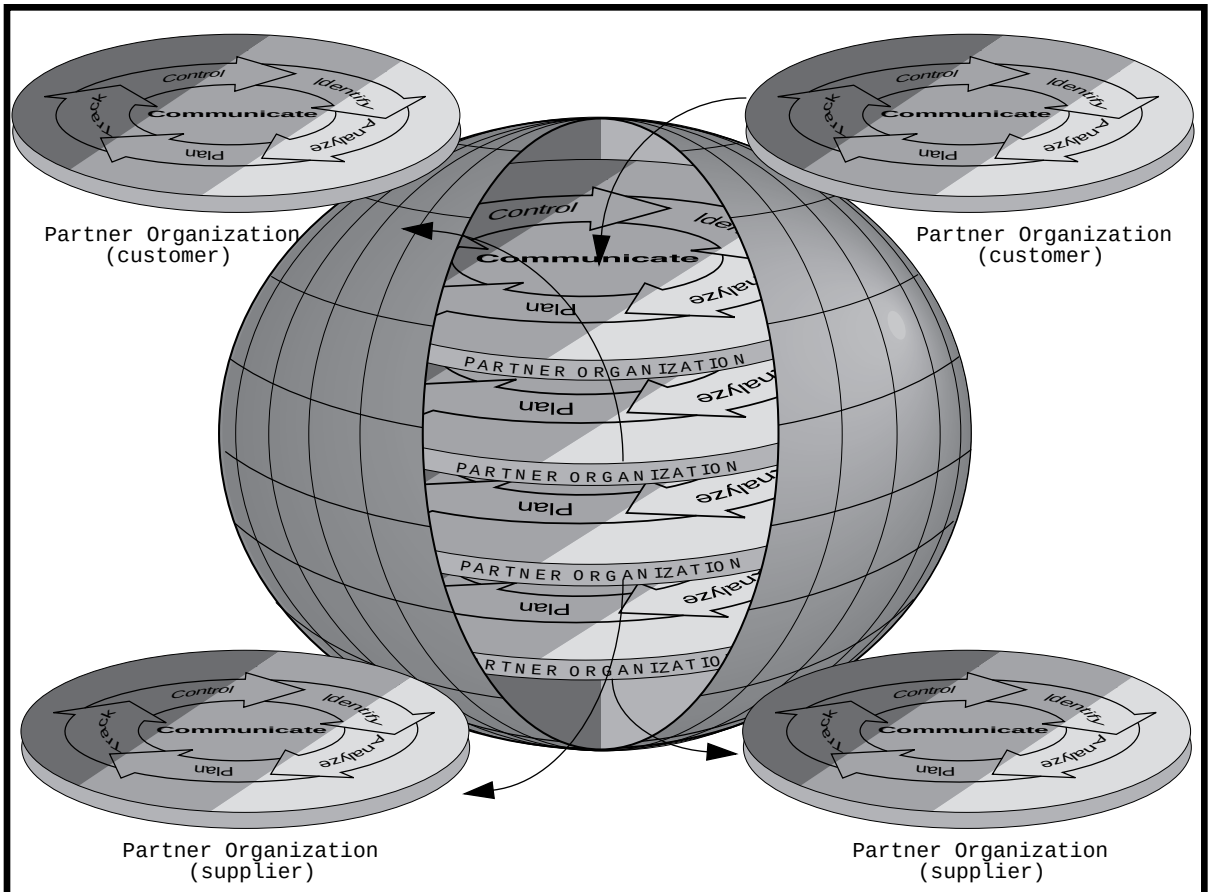


Figure 3-3: The Team Risk Management Process Sphere

4 Team Risk Management Processes

The team risk management processes shown graphically in Figure 4-1 include continuous processes and a one-time process activity, the baseline risk assessment. The continuous processes of team risk management incorporate all five steps of the SEI paradigm (shown in Figure 3-1) into four processes by combining the identification and analysis steps into the routine risk identification and analysis process. Similarly, the baseline risk assessment combines the identification and analysis steps of the paradigm into a single process activity that establishes the initial set of risks and initiates the continuous process activities. The team review process defines cooperative risk management activities between the partner organizations.

The baseline risk assessment is an intra-organizational process executed independently by each partner organization (government and contractor) involved in team risk management. The team review process is an inter-organizational process conducted jointly between the government and the contractor. The other continuous risk management processes are dual-role (implemented as both intra- and inter-organizational) processes.

The nine principles of team risk management and the cooperative team approach provide the foundation for all of the team risk management activities, whether intra-organizational, inter-organizational, or dual-role activities. Thus, while the inter-organizational processes are inherently team activities, the intra-organizational and dual-role processes also have a strong team character. This sense of “team” pervades all facets (processes, methods, and tools) of the implementation of team risk management.

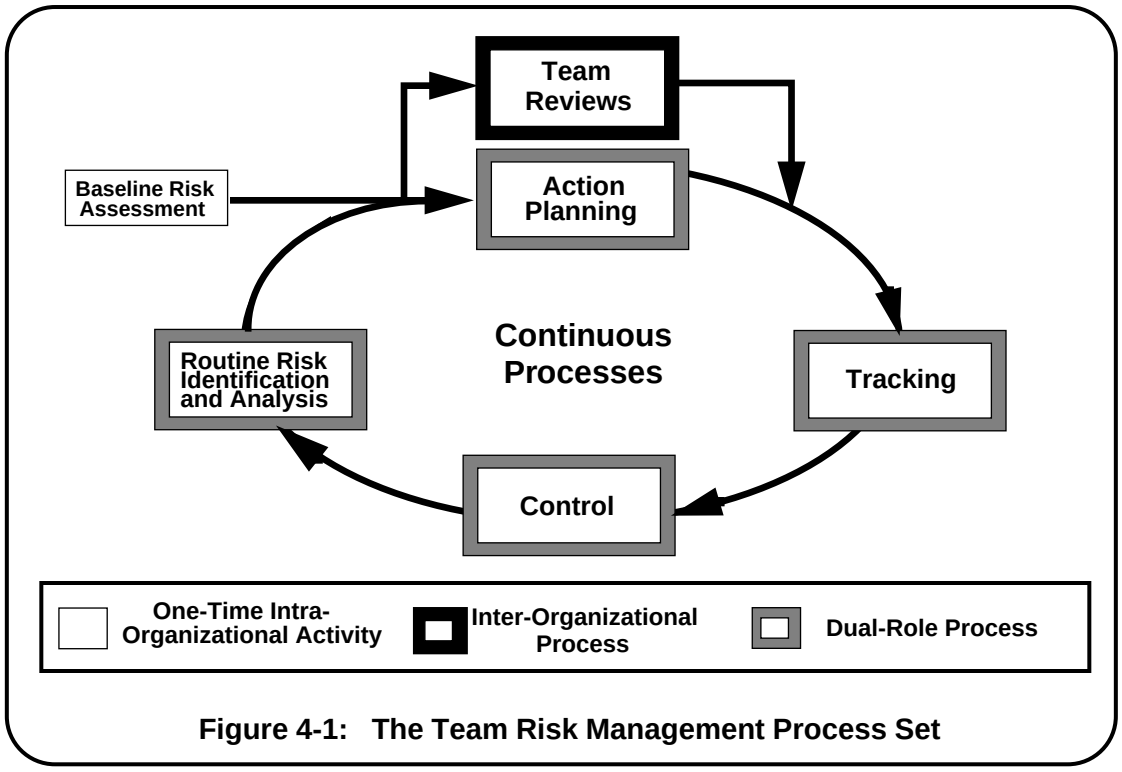


Figure 4-1: The Team Risk Management Process Set

The basic classifications of team risk management processes are summarized in Table 2.

Classification	Description
1. Continuous processes	the dual-role continuous risk management processes consist of the SEI risk management process steps: identification, analysis, planning, tracking, and control as well as inter-organizational activities, including regularly scheduled team reviews as well as unscheduled informal meetings and communications
2. Baseline activities	the initial, one-time identification and analysis of activities that establish the baseline set of risks conducted by each partner organization, government and contractor

Table 2: Process Classifications of Team Risk Management

When team risk management is applied to a software-dependent development program that has been awarded by the government to a prime development contractor, both the government office and the contractor concurrently execute the team risk management processes. Specifically, each conducts a baseline assessment and subsequently executes the continuous team risk management processes. This concurrent activity is shown graphically in Figure 4-2.

The team reviews held throughout the life of the program provide formal inter-organizational communication and coordination on program risks. These joint government and contractor reviews include reviews of the status of risks, discussions of the risks, risk management activities and plans, and reviews of strategies for dealing with risks. Through these team reviews the government and contractor share perspectives, ideas, and objectives and arrive at a better understanding of the program risks and objectives. These reviews are generally scheduled as part of routine program reviews but can be convened as needed to address specific issues or as part of a key program milestone.

The baseline assessments establish the initial risk sets: one for the government program office and one for the contractor. The risks identified in the baseline form the basis for the initial team event, the team review. This review combines the most important risks from both the government and the contractor into a program-wide list, the Joint List of Risks. (The number of risks included in the list is program dependent but generally ranges between 10 to 20.) The Joint List of Risks is the focus of the joint “team” management efforts and represents the most important risks faced by the program.

In addition to being the basis for establishing the initial Joint List of Risks for the program, the baseline risk assessments also identify risks that are managed individually by the government and by the contractor. Each organization manages its risks through the continuous process loop activities, as shown in Figure 4-1 and Figure 4-2.

Following the baseline assessment, action planning is initiated. The action planning process defines and initiates specific actions (strategies) for dealing with the risks. The tracking and control process steps monitor the results of the action plans and control the progress of the

program's risk management activities. The routine risk identification and analysis process step is a continuous activity, throughout both the government and contractor organizations, that identifies new or changing risks in the program. All risks are incorporated into the action planning process, and are incorporated into the team review process as required.

Team risk management is implemented as a routine, continuous, and integral part of program management activities. Within this program context, it provides the basis for joint (government/contractor) management of program risks as well as the basis for individual organizations to manage risk. Each of the team risk management processes is described in more detail in subsequent sections of this document.

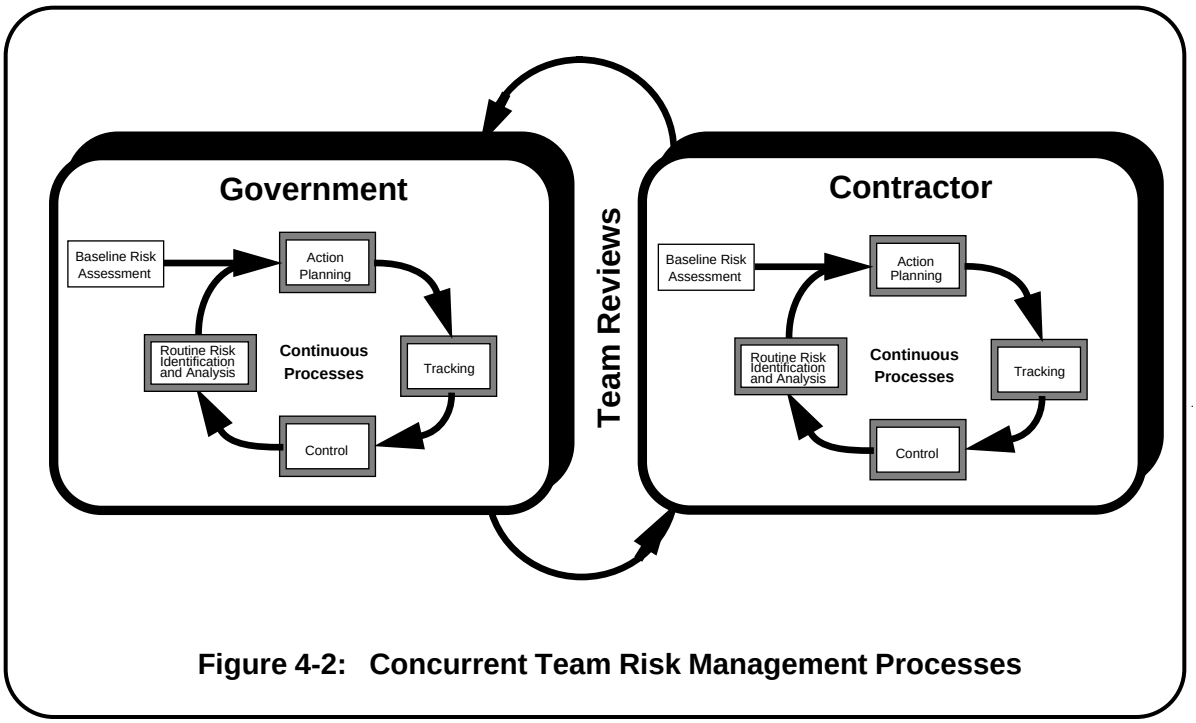


Figure 4-2: Concurrent Team Risk Management Processes

4.1 Continuous Team Risk Management Process Overview

Risks exist and emerge throughout the entire life cycle of a program; thus, the processes of identifying and managing risks must continue from the program's inception. The continuous processes of team risk management, as depicted in Figure 4-1, comprise a cyclic set of routine activities for managing risk. Collectively, these processes involve: identifying risks, periodically reviewing and analyzing new risks, planning for the judicious application of resources to mitigate risks, tracking the status of risks and risk mitigation actions, controlling risks that turn into problems, and communicating about risks among all partners in the program. The systematic methods that make up continuous team risk management processes can be adapted to any program's infrastructure and culture through the modification of forms or instruments, the ap-

propriate scheduling of activities, the integration of the methods into existing program activities, or the adoption of the complete, unmodified set of processes, methods, and tools.

This section addresses the continuous aspects of team risk management. Section 4.2 discusses the initiating activity of the team risk management process, the baseline risk assessment, which establishes a baseline set of risks for the program and is the preliminary activity for continuous risk management.

The primary cycle of activities in continuous team risk management has five parts as listed below and as briefly described in Table 3:

- Routine risk identification and analysis
- Team reviews
- Action planning
- Tracking
- Control

All of the activities are tied together through informal and formal communication processes. These activities enhance the cooperative interactions and trust between partners and team members, and build and reinforce the shared program vision required for effective team risk management.

Team Risk Management Process	Methods/Tools	Communication Characteristics
Routine Risk Identification and Analysis	• routine risk form processing • periodic risk reporting • periodic individual interview session • periodic risk assessments	• non-judgmental • non-attribution • confidential • individual voice
Team Reviews	• comparison risk ranking • nominal group technique	• mutual understanding • consensus
Action Planning	• periodic technical reviews • review and assign • strategize	• mutual understanding • consensus on responsibilities
Tracking	• metrics • status indicators • triggers	• mutual understanding
Control	• risk corrections • risk action	• mutual understanding • consensus on actions

Table 3: Continuous Team Risk Management Methods, Tools, and Communication Characteristics

Except for team reviews, all of the continuous team risk management activities are included in a “core cycle” of processes. Team reviews provide the means for the government and the

contractor to jointly decide on risk plans, responsibilities, and actions for managing risks, and for formally communicating information on the current progress of risk management activities in their respective organizations. Team reviews, then, are a method that can be viewed as being on the surface of the team risk management sphere (Figure 4-2), whereas the core cycle of activities–routine risk identification and analysis, action planning, tracking, and control–embody the risk paradigm processes and constitute the center of the team risk management sphere.

The core cycle begins with routine risk identification and analysis to identify new risks, proceeds to action planning for those risks, and is followed by the tracking and control of those risks. These activities are sequential for a given risk, but are continually overlapping program activities in that there will always be risks in any one of these phases. (There is one exception when a baseline is established. This exception will be discussed later.) Routine risk identification and analysis provides the means to identify new risks during the program's life cycle and to perform a preliminary analysis on these risks. This can be on a voluntary basis where new risks are identified at any time by any person, but also includes periodic, more formal, reviews (assessments) of the program by a select set of knowledgeable personnel. Regardless of the specific method used, this process is a combined identification and preliminary analysis which results in a:

- Risk statement
- Context
- Preliminary analysis that includes:
  - estimation of significance (of the impact)
  - estimation of the likelihood of occurrence
  - estimation of the time frame of occurrence (or need to take action)
  - an indication of criticality (i.e., requires immediate management attention)
  - and (optionally) a recommendation for resolution

Other analysis methods can also be used, particularly to provide a more quantitative analysis of risks. The other analysis methods are part of the ongoing development activities within the SEI risk program.

A result of an identification and analysis process in which at least one risk is identified is the creation of, or the addition to, a list of risks referred to as the Master List of Risks. For a government/contractor implementation of team risk management there are two lists, the Government Master List and the Contractor Master List.

As part of the team review process, the Joint List of Risks, which contains the risks being managed on a joint basis, is created and managed. Selected risks from each of the master lists are included in the Joint List of Risks for the program. The risks included in this list are risks

considered to be the most important risks to the program. The relationship between the lists is shown in Figure 4-3.

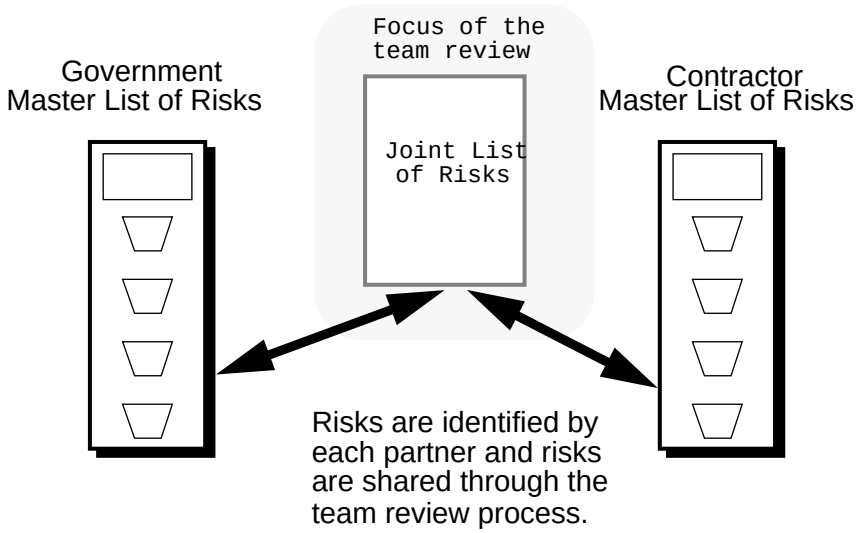


Figure 4-3: The Relationship Between the Lists of Risks

As part of the planning actions for risks, newly identified risks are reviewed on a periodic (e.g., weekly, bi-weekly, monthly, etc.) basis and assignments are made specifying responsibility for the risk. These same periodic technical reviews are also the means by which the status of existing risks and action plans can be reviewed. Action planning continues with the determination of some immediate action or the decision to investigate the risk in-depth and develop detailed mitigation strategies. If detailed mitigation strategies are needed, these are evaluated based upon their costs, benefits, and significance to the program before being approved and implemented.

Any risk may require tracking and control, either because tracking is the only activity being undertaken for that risk or because mitigation strategies are being put in place. Tracking provides the means to keep the responsible management personnel, as well as the program manager, aware of the current status of the risks and the mitigation strategies. Tracking measures the progress of the factors associated with a risk, which provide indications as to the probability of its occurring, changes in impact to the program on occurrence, and changes in the time frame (e.g., a risk was not expected to turn into a problem until next year, but indications are that it will now occur in the next few months). Depending upon the desired actions when risk indicators reach pre-defined triggers, some type of controlling activity occurs. This can range from taking immediate action to re-evaluating the situation and developing alternative plans.

Finally, there are risks identified by either partner that are important enough to require joint attention, review, or management by both partners, government and contractor. The team review is the forum for the exchange, review, discussion, and prioritization of a joint set of risks.

This can be held on a quarterly basis or associated with other milestone progress reviews of the project. Risks discussed in this forum may become the responsibility of either partner individually, or can become joint risks that are managed through the efforts of both partners. The team review is a formal, regularly scheduled meeting. Continuous, less formal communication on the progress and status of risks and risk mitigation strategies is also an integral part of team risk management. It is through these informal communications that much of the information relative to risks and their management is transferred between both parties.

In subsequent parts of this section each of the processes of continuous team risk management is discussed in greater detail.

4.1.1 Routine Risk Identification and Analysis

Routine risk identification and analysis involves the participation of personnel throughout the organization and combines the processes of identification and analysis into a set of distinct team risk management activities. The methods which can be employed in routine risk identification and analysis are summarized in Table 4.

Method	Description	Characteristics
Routine Risk Form Processing	Routine distribution and processing of risk forms, submitted by program personnel as risks are identified	• individual input • continuous • anonymous
Periodic Risk Reporting	Periodic (scheduled) reporting of risks by program personnel	• individual input • periodic scheduled event
Periodic Individual Interview Sessions	Periodic interviews of individuals throughout the program	• individual input • periodic scheduled event • confidential • non-attribution
Periodic Risk Assessments	Abbreviated versions of the baseline risk assessment which are held periodically based upon time milestone events	• peer group • periodic scheduled event • confidential • non-attribution

Table 4: Routine Risk Identification and Analysis Methods

Routine Risk Form Processing

The implementation of the routine risk form processing method is accomplished through the broad distribution of risk forms. The risk form enables any individual within the program to identify a risk, to provide support information regarding the risk, and to complete a preliminary analysis of the risk. When a risk form is received, it flows into the action planning processes as shown in Figure 4-4. The risks are reviewed periodically as part of the action planning process, but if a risk is marked as critical, it is given immediate attention.

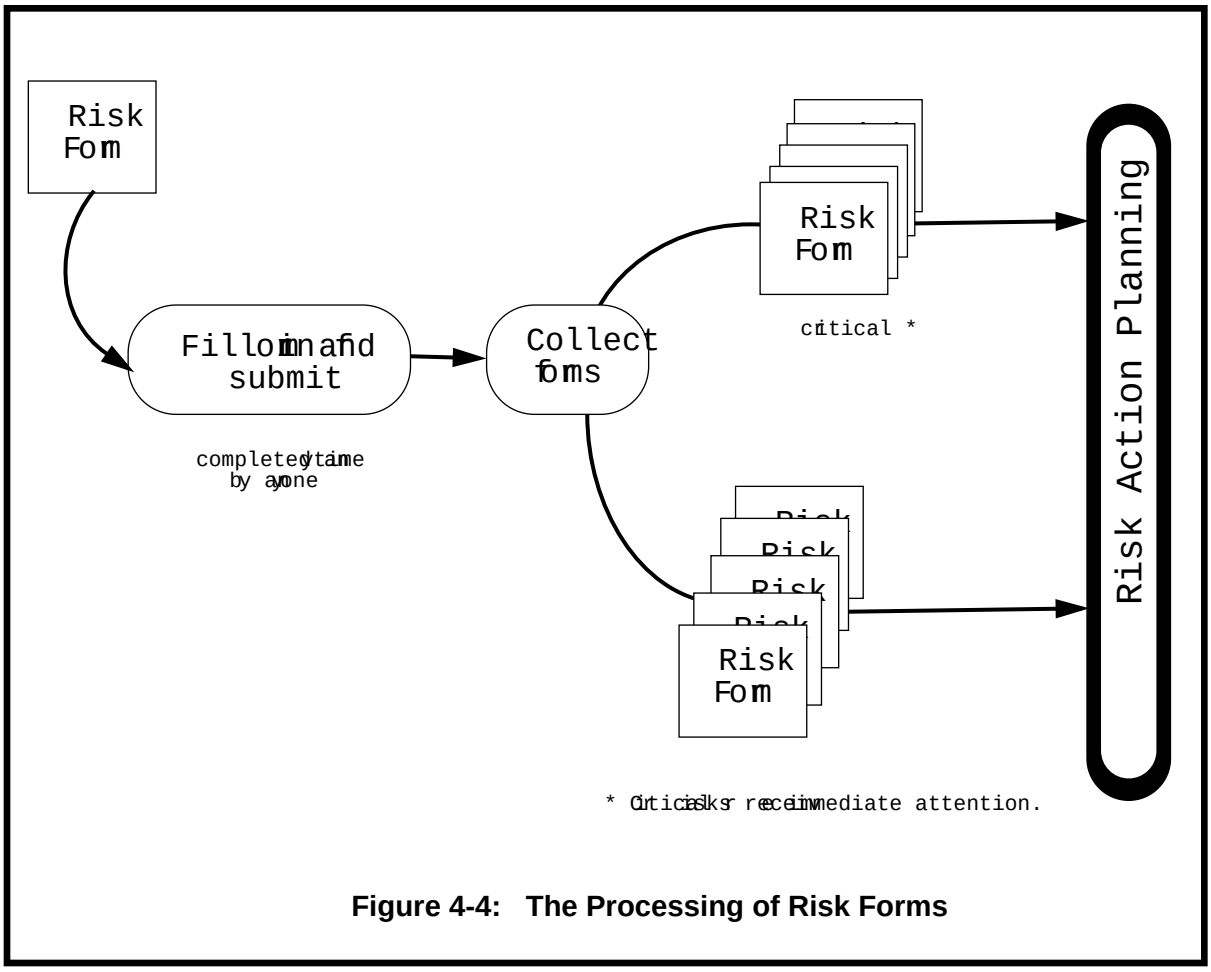


Figure 4-4: The Processing of Risk Forms

The Risk Form, as shown in Figure 4-5, asks individuals to write down what they consider to be new risks or changes in known risks that the program faces. They may include additional details on the conditions or other factors that are relevant and significant. This is the context of the risk; this information is used to better understand the issues relating to the risk and will provide additional support for managing the risk within the program.

Next, they are asked to evaluate each risk in terms of its potential impact on the program, its likelihood, the time frame, and its criticality. Checking ***Significant*** implies serious impact to the program. Checking ***Likely*** means the risk impact is more likely to occur than not. Checking ***Near-Term*** means the impact is likely to occur in a near-term time frame or action to mitigate the risk must be taken in the near-term (a long lead-time item). Checking the ***Critical*** box indicates that the risk may be a showstopper or threatens program success. Risks marked critical are immediately addressed and elevated to the appropriate program personnel.

There is space provided to capture a possible recommendation for dealing with this risk. This information is not required, but, if captured, provides additional information that may be helpful in resolving the risk.

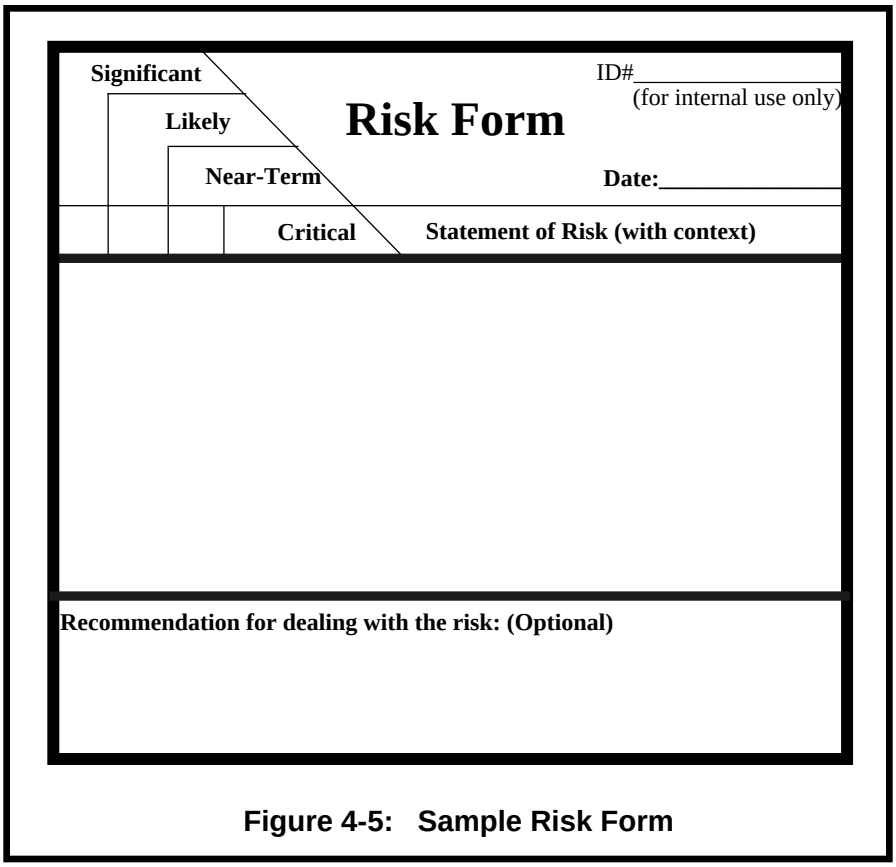


Figure 4-5: Sample Risk Form

Completed risk forms are generally submitted anonymously to the appropriate individual coordinating risk identification activities. In some programs, particularly in risk-aware cultures [SEI 92], forms are submitted directly to management personnel without the need for anonymity. In these environments, risks and risk management are viewed as normal parts of routine program activities.

To foster the continued vigilance required for effective risk management, program personnel are reminded of the routine risk identification process as part of the discussions of risk issues held during regularly scheduled program meetings. During these discussions they are encouraged to maintain vigilance as the program evolves and to submit the risk forms as soon as a new risk is identified. This continued communication on risk issues, which we refer to as risk awareness, is crucial for the effective identification and management of risks.

Periodic Risk Reporting

A second method for routine risk identification and analysis involves the periodic reporting of risk identification information. These risk identification status reports are generally included as part of the program's normally scheduled reporting activities and may involve every individual or only selected key individuals working on the program. This method asks that weekly, biweekly, or monthly, each individual involved in the program submit a risk identification status report as part of routine status reporting. The risk identification status report may be the risk form or a summary risk identification section included within the program's normal status re-

port forms (see Table 5). The risk summary section should consist of a risk statement and its significance, likelihood, time frame, and criticality. If an individual has not identified a new risk then that information should be reported as well.

Prior to the scheduled submission of the risk report, each individual on the program reviews the current listing of risks and the taxonomy summary [Carr 93] that is printed on the reverse side of the risk form to determine if conditions have changed such that a new risk has emerged. Based upon the results of the review, the risk identification report (risk form or summary) is submitted.

The periodic individual review of the conditions of the program and submission of the risk report are important parts of effective routine identification and analysis of risk.

Report Type	Description	Submission
Risk Form	The Risk Form is completed for each identified risk. If no risks have been identified, the form is marked "None Identified."	The completed form is submitted as part of the periodic program development and status reporting processes, e.g. biweekly technical status meeting, monthly program status meeting.
Risk Identification Summary	A section of a program status report that includes the following information on newly identified risks: • Risk statement • Significance • Likelihood • Time frame • Criticality • Context	The summary report is included in the program status report.

Table 5: Periodic Risk Identification Status Reporting

Periodic Individual Interview Sessions

In addition to the routine distribution and processing of risk forms, periodic risk identification interviews of program personnel can be employed as an additional method for routine risk identification and analysis. These interview sessions provide a stimulus to the overall identification activities, provide an opportunity to formally re-assess the risk condition of the program, and foster a risk-aware culture. These activities are especially important during the transition phases of the implementation, where the team risk management approach has not yet been institutionalized into the organization.

The periodic individual interview session consists of a series of one- hour interviews conducted by a trained individual from outside of the program, but from within the same corporate en-

vironment. Ideally, this is an individual dedicated to process improvement, risk management, or other non-project-specific assignment. Alternatively, a third-party organization may conduct these sessions. During the transition period in adopting these methods, the SEI supports the interview sessions through direct involvement in the sessions or through training of the session interviewer.

Scheduled periodically (for example, quarterly), the interview sessions are grouped into sets of six to ten and are conducted over a one-or two-day period. Each interview session requires the participation of one individual from the program and consists of questions asked of that individual by the interviewer. Personnel are selected based upon their technical knowledge of the program and their willingness to share their views on program issues.

Periodic Risk Assessments

Periodic risk assessments are abbreviated versions of the baseline risk assessment which is described in Section 4-2 of this document. These assessments are held periodically throughout the life of the program and consist of a series of interview sessions that identify risks that exist in the program. These assessments provide additional insight into program risks and can be used to support critical decision points in the program. The specific schedule for these events is based upon the individual program's size, duration, objectives, and related management measures to best meet the needs of the program. They are planned at specific times throughout the life of the program or are conducted as part of key program milestone events.

The information provided through a periodic risk assessment, periodic individual interview, risk identification summary report, or a completed risk form is exactly the information that is generated for each risk identified in the baseline risk assessment. Thus, the risk information content and flow is the same throughout the team risk management processes, whether a risk is identified during the continuous identification and analysis processes or during the baseline risk assessment. All of these risks are included in the Master List of Risks and are processed through action planning. In the next section, we discuss how selected risks are used in the team review process.

4.1.2 Team Reviews

The team review is a joint meeting of the government and contractor program managers and their immediate staff to discuss and prioritize risks. It brings together each program manager's list of current top risks, maintains continuity between these risks and those that were most important at the previous meeting, assures that there is a common understanding of the most important risks to the program, and assigns new action items. Its purpose is to build and maintain momentum in government/contractor team risk management.

Nominally, the meeting is held quarterly, although another time basis can be chosen to suit a particular program's needs. It is ideal for the team review to be held in conjunction with or just before a program status or design review meeting between the government and the contractor. The team review provides a time-effective review of the key risks to the program, with all

the advantages of open exchange of information; it also sets the stage for an improved and focused general program review meeting.

Each program manager will have the list of prioritized risks, the Joint List of Risks, from the previous team review meeting; this list will be the starting point for the team review. However, new risks will also have been identified in the organizations through the routine risk identification and analysis process. From these new risks, each program manager will select candidates for inclusion in the Joint List of Risks on the basis of responses to three questions:

1. Which of these new risks informs the other party of a serious risk that they should be aware of?
2. Which *may* need to be transferred or delegated to the other party?
3. Which will require joint action to resolve?

The team review process is depicted in Figure 4-6. The team review opens with a review by each program manager of the current status of all risks and action items from the previous team review. Risks may be deleted from the list (because they have been resolved, for example, or because they are no longer viewed as sufficiently important), but this is accomplished by agreement between the two program managers. Only if both program managers agree are risks closed. Next, candidate new risks (and their context information) for inclusion on the list are reviewed.

In the first occurrence of the team review, where no Joint List of Risks exits, each program manager selects approximately to 5 to10 risks from their respective Master List of Risks to be included in the first version of the list. The specific process steps within the team review are modified, as needed, to address the fact that a Joint List of Risks did not exist prior to the current team review, e.g., the old list is not reviewed.

The next step in the ranking process is to agree precisely on the comparison criteria. The risks are compared on the basis of which is “more important” to the program, but “importance” can have many dimensions, such as cost, schedule, and fitness of the final product. Before being confronted with specific choices of risk, the participants agree on the factors that will be considered during the ranking process. This step helps provide all participants with a common, shared understanding of the risks prior to ranking.

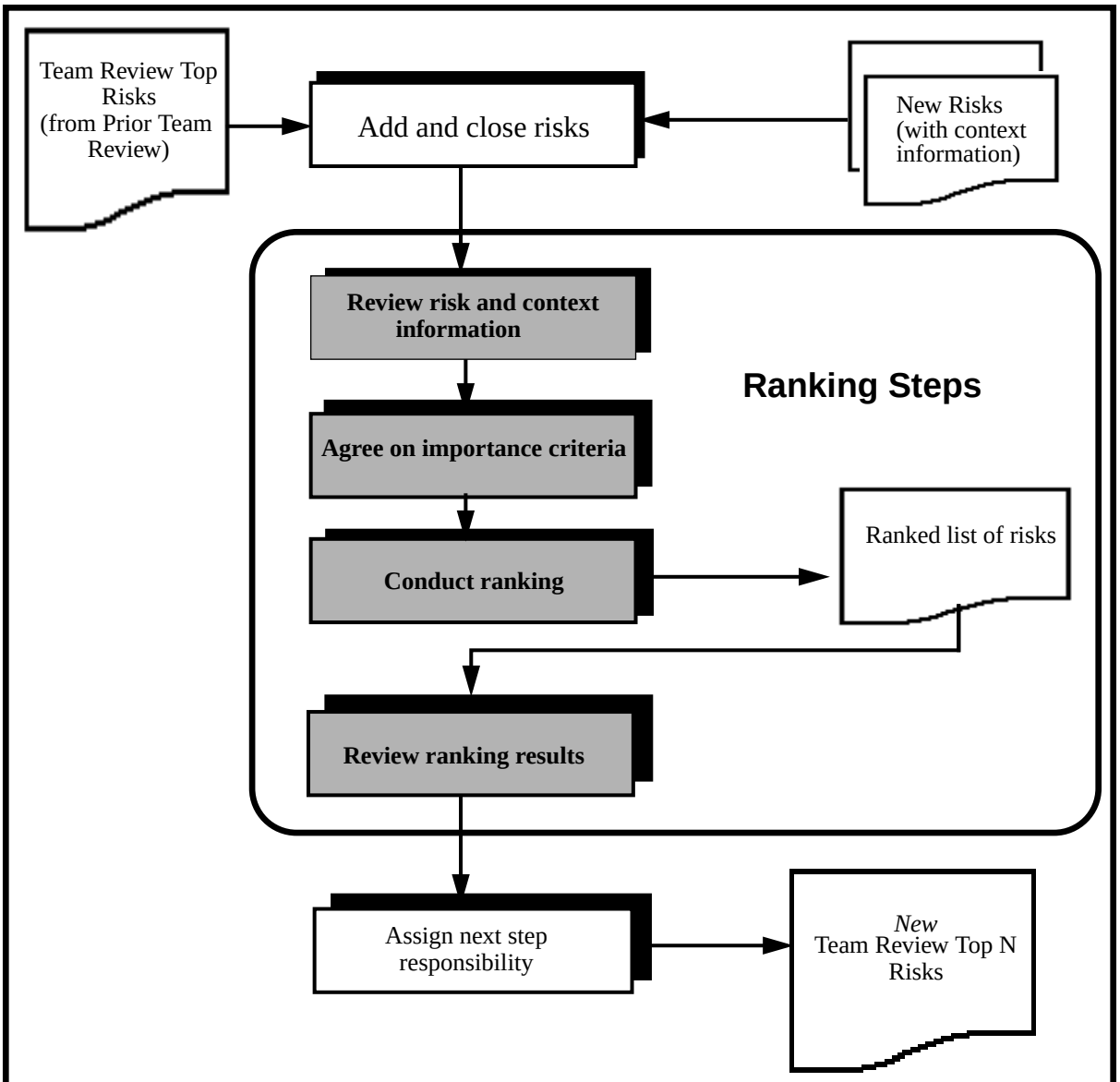


Figure 4-6: The Team Review Process

The purpose of the conduct ranking step is to sort the list from the “most important” to the “least important.” As part of this process, each risk statement and associated context information is read and reviewed. Discussion among all the participants leads to a final prioritized list of the attributes they will use to evaluate which risk is “more important” to the project. The ranking is accomplished using any of several methods, two of which are Comparison Risk Ranking (CRR) [FitzGerald 90] and the selection process of the Nominal Group Technique (NGT)

[Scholtes 88]. Both of these methods provide the needed rank ordering and achieve the shared understanding that is desired.

Regardless of which method is used to achieve a final prioritized list, the participants in the team review then systematically review the finished list, agreeing on action items to be carried back for resolution by the two partner organizations. The risks can become the responsibility of the government, the contractor, or both—risks requiring joint actions by the partners. Thus, either party may acquire new risks from this process as well as transfer risks to the other party.

The product of the team review session is a ranked list of risks tagged to identify responsibility for pursuing action (government, contractor, or joint action) known as the Joint List of Risks. See Figure 4-7 for an example. At the end of the initial team review session, each party shares an understanding of the top 15 to 20 risks for the program and holds a list of action items agreed to during the subsequent discussion.

Rank	Risk	ACTION		
		Government	Contractor	Joint
1	Risk 1	✓		
2	Risk 2		✓	
3	Risk 3			✓
4	Risk 4			✓
5	Risk 5		✓	
⋮	⋮			

Figure 4-7: Sample Team Review Joint List of Risks

One result of the team review is the transfer of new risks into a partner organization. These risks are added to the organization's Master List of Risks and are input into the action planning process as shown in Figure 4-8.

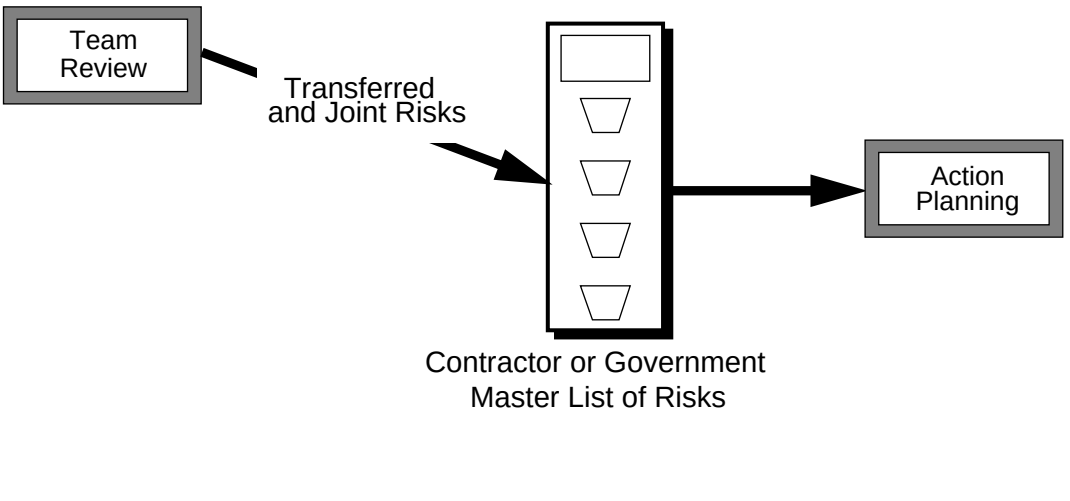


Figure 4-8: Disposition of Transferred and Joint Risks

4.1.3 Action Planning

Action planning for risks is the determination and implementation of actions necessary to manage a program's risks. This is where the integration of risk management processes with existing program management becomes most evident. Planning, in general, is an integral part of program management, whether planning how to meet specific milestones or determining the best design strategy for meeting specified requirements. Risk planning requires a systems perspective to maximize the effective use of scarce resources within a program. Planning the mitigation of risks is a proactive means of minimizing future problems [Dorofee 93].

Actions range from accepting the risk (do nothing) to developing strategies requiring task plans, schedules, WBSs, etc. The key to planning for risks is to make as effective and efficient use of resources as possible to reduce the overall risk while maximizing the potential for gain to the program.

Strategies for the most important risks are generally planned first. Plans for other risks should leverage off these strategies for maximum return on investment in risk mitigation strategies (e.g., greatest reduction in risk exposure for the least expenditure of resources). All risks are reviewed, but only those that are important to the program will have any significant amount of resources expended on them. In general, it is not practical to assume that all risks can be eliminated or significantly reduced. Many will be accepted, while many others will merely be watched and acted upon if conditions change.

Risks are reviewed by management with the most critical risks reviewed at the top level of management – the program manager or a specifically designated review group, such as a risk management board or risk council. This technical review is a periodic activity that not only ad-

dresses new risks, but also reviews the status of existing risks. Less critical risks do not need the full attention of top level management, but visibility into those risks can be provided if desired. Once reviewed, risks are then assigned throughout the organization to be dealt with by the appropriate personnel. Action planning, then, is a repetitive or cyclic process carried out throughout the organization. Plans to manage risks can be developed and approved at any level, as management delegates the effort and authority to deal with risks to the appropriate level within the organization. Plans for the more important risks to the program are likely to be managed at the program manager level or jointly at the government/contractor team level. A systematic approach to planning ensures the appropriate visibility and delegation of responsibility.

Action planning is shown in Figure 4.9. There are two basic phases in action planning: *review and assign* responsibility and *strategize*. The first step is performed as part of a periodic technical review by a responsible organization or individual to determine which risks can be dealt with easily and which ones will require (and justify) expenditures of time and effort to develop detailed analyses and strategies.

Review and Assign

The Review and Assign process step is the logical first step upon identification of a risk. Once a risk has been identified, then a decision is made regarding what to do with it, and who will be responsible for it. This activity occurs after a risk has been identified and is accomplished by an individual or organization with a total project perspective, such as the program manager or the risk management board. During a review, it is possible to identify and decide upon actions for some risks, while others may need further investigation or consideration before action can be taken. Also, there will be risks which are appropriate to delegate and can be handed to others to manage. Regardless of the type of action decided upon at this review, an assignment of responsibility is made for each risk. At the end of this review and assign activity, designated actions are carried out and recorded for each risk.

New risks are reviewed on a periodic basis during routine periodic technical reviews, unless they are designated as critical. Critical risks are reviewed immediately.

Periodic Technical Reviews. Periodic technical reviews are internal meetings held to review and assign responsibility for new risks, to review status, and to assess the progress of risk mitigation strategies (see Tracking and Control, Section 4.1.5, for more on risk status). The key element is that the review process occurs and is accomplished through methods consistent with the program's routine program management activities.

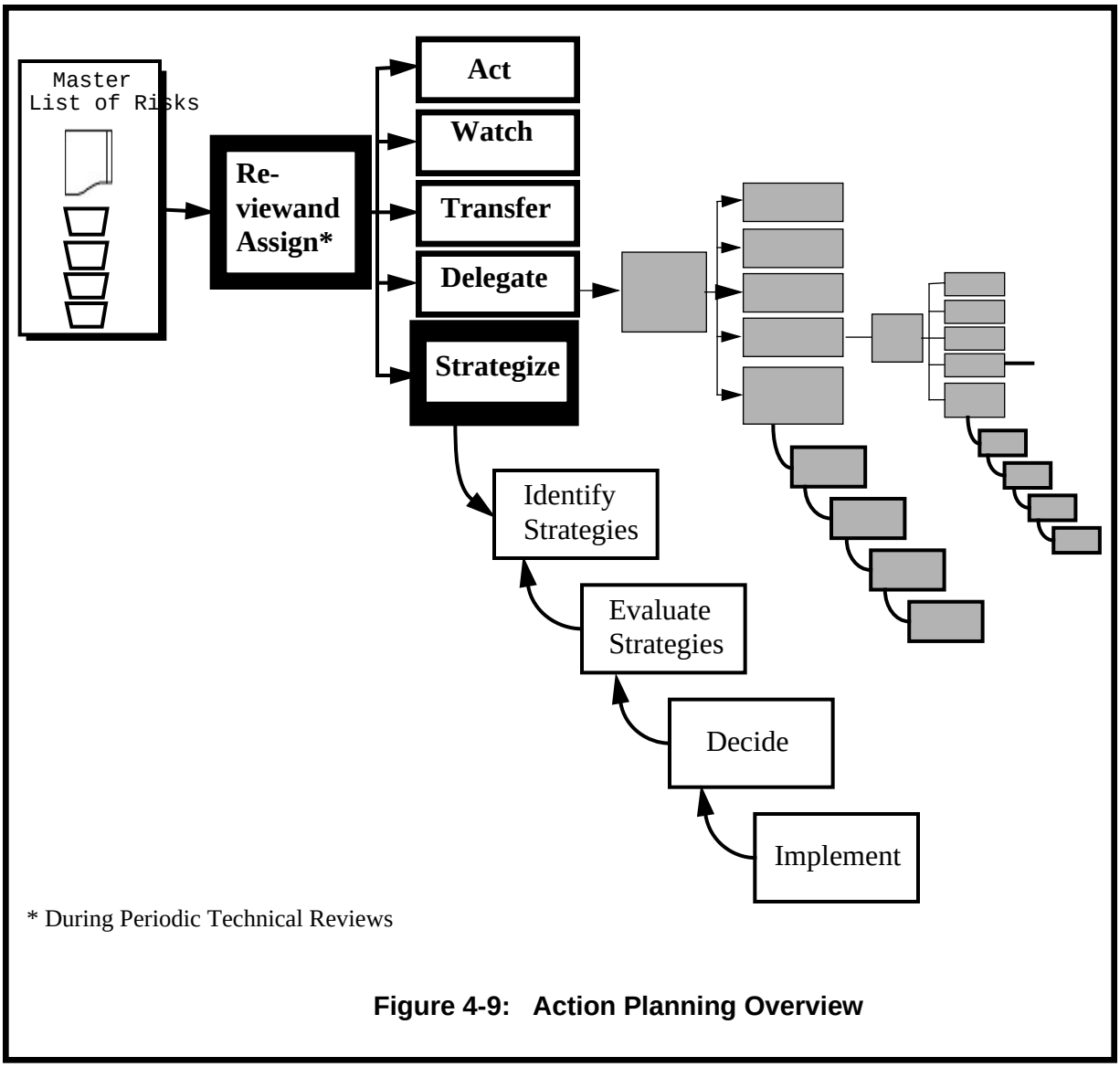


Figure 4-9: Action Planning Overview

New risks are identified from routine risk identification and analysis, transferred from other organizations (e.g., from government to contractor via a team review), or identified as part of a baseline risk assessment. Routine risk identification and analysis identifies new risks that need to be reviewed and assigned to someone to manage. The review and assign activity is also required for baseline risks and may be done incrementally due to the typically high number of risks identified at that time. Based upon the needs of the program, a specifically chartered risk management board may be assigned responsibility for reviewing risks. The periodic technical reviews could be a part of routine program reviews or the board may hold its own periodic meetings. In either case, these meetings are “internal” to each partner’s organization. The result of these meetings is the determination of action(s) and the assignment of person(s) responsible for carrying out the action(s).

As each risk is reviewed, an initial determination of a type of action is made. A responsible person (or organization) is assigned the action and the responsibility to report status back to the reviewing organization (e.g., risk management group) or manager. The action decided upon, as well as the responsible person and other pertinent data (such as a due date, etc.) are documented along with the other risk information (statement, context, significance, etc.). Risk information can be maintained in a data base, or paper format, etc., depending upon the resources and requirements of the organization. The important factor is that the risk information is kept, that it provides meaningful data to program management, and that it is accurate. From this point on, additional information is gathered and added as the risk moves through risk management activities. Once the review and assign process step is complete, the responsible person carries out the designated action.

Types of Actions. When reviewing a risk, there are five likely types of actions that can be decided upon immediately:

- Act
- Watch
- Transfer
- Delegate
- Strategize

The first four are decisions on the disposition of the risk that can be made with current information and usually with little or no additional resource expenditure. Strategize is a process step that involves some expenditure of resources to perform. Table 6 describes each type of action.

Strategize

Figure 4-10 provides an overview of the Strategize phase of risk action planning. Strategizing is a matter of identifying possible alternative strategies, evaluating those strategies for maximum benefit, deciding upon the appropriate strategies, and implementing them.

There are four basic types of strategies:

- Research
- Accept
- Eliminate
- Reduce

A combination of any of these strategies is also possible (e.g., perform research into the effectiveness of alternative designs while taking minor action to reduce the risk as well). Strategies to eliminate or reduce a risk can include action(s) to take in the near-term or future. Future actions, or contingency plans, address actions to be taken when resources are available, a trigger event occurs, or when the risk becomes a problem. Table 7 provides details of each

strategy. It is also possible that upon reflection, it is decided that a detailed plan is not needed and that one of the previous types of actions (act, watch, etc.) would be more appropriate.

Action	Description
Act	These risks are easily resolved by a quick-response or rapid turnaround type of action that requires little or no expenditure of resources. In this case the reviewer is prepared to make an immediate decision based on current information. These risks are immediately **acted** on. For example, a programmer's concern with a perceived lack of a catastrophic backup procedure can be alleviated with a letter informing all employees of such a policy and explaining it. Actions and relevant responsibilities for those actions are noted with the risk information and status reports.
Watch	These risks are to be **tracked**, but expenditure of resources for any other type of action or investigation is not warranted at this time. For example, given a remote risk that a subcontractor tool may not be available, the progress reports from that subcontractor can be monitored for indications that the schedule is slipping. The means of tracking and the trigger events are noted with the risk information.
Transfer	These risks are identified by an organization but the authority and accountability to actually deal with the risk lies elsewhere. For example, a contractor may identify a risk that can only be dealt with by the government, such as availability of government supplied equipment. Such risks are **transferred** to the other organization. Some reporting of status to the transferring organization may also be requested. Note that a successful transfer requires acceptance on the part of the receiver. A team review is one appropriate venue for transferring a risk. Also, a risk can be transferred up or laterally within the organization.
Delegate	There will be risks more appropriately addressed within another part of the organization. For example, a risk may be better handled by someone in the software testing area as opposed to the software manager. These risks are **delegated** down the chain of command to another person (or organization). The planning process is repeated by that person, starting with the review and assign responsibility step. Reporting of status may also be requested to maintain visibility to management.
Strategize	For these risks, resources are needed to either further investigate the risk itself or to develop **detailed strategies** and schedules for mitigating actions. Alternative strategies are identified, evaluated, selected and implemented. Strategies can be implemented in the near-term, or developed for use as contingency plans.

Table 6: Review and Assign Action Types

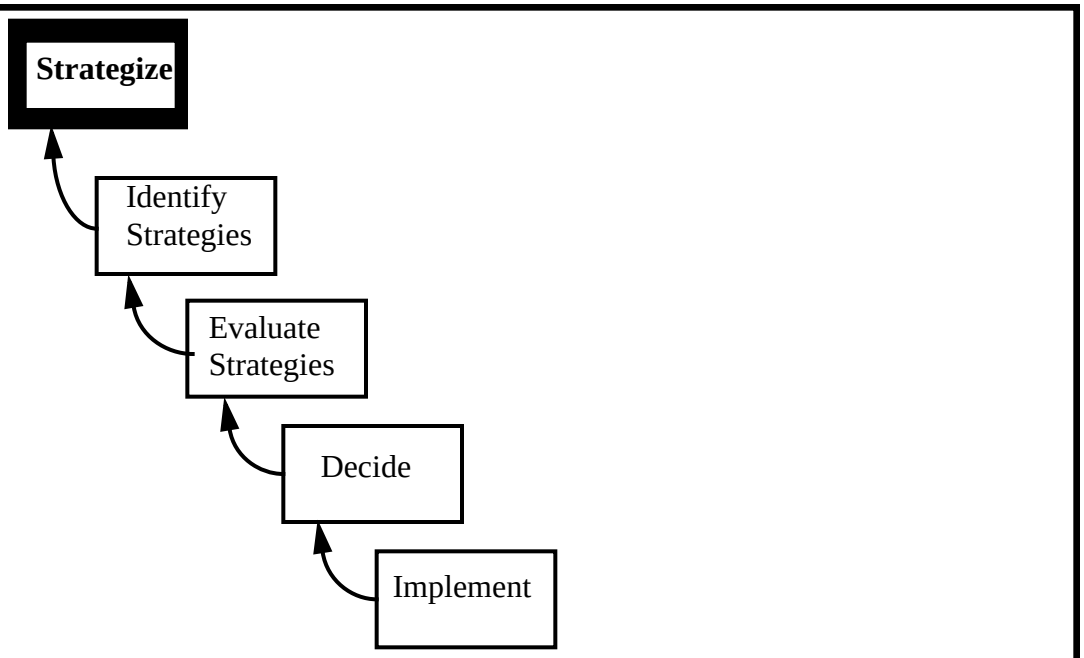


Figure 4-10: Strategize Overview

Identify Strategies. Strategies can be identified through any number of existing problem-solving techniques, such as Xerox's method [Xerox 92]. Each viable alternative strategy should include, as a minimum:

- description of actions to be taken
- estimate of required resources
- estimated schedule
- estimated benefit or change in the state of the risk (e.g., less impact on occurrence)
- known relationships or dependencies to other alternative strategies (e.g., strategy B enhances the results of strategy A if both are used)

Evaluate Strategies. The alternative strategies can be evaluated to determine which one has the best potential for managing a particular risk. For a particular risk, for example, which strategy:

- provides the greatest reduction in risk?
- requires the least resources?
- requires available resources (as opposed to unavailable)?
- has the least impact on schedule?

Tables or matrices can be constructed to evaluate the strategies for a given risk, if the choices are complicated. Evaluation can be done on a qualitative basis, but there will be a high degree

of subjectivity and dependence on the expertise of the evaluators. Quantitative evaluation would provide more accuracy but the cost (and precision) of quantitative measurements of benefit and cost often require considerable resources.

Strategy	Description
Accept	**Accept** the consequences of it happening–essentially, do nothing. These risks are not tracked. They are documented and put aside. If the risk becomes a problem, it is handled as a problem. This is an appropriate strategy for those risks which are simply not worth the effort to deal with. Changes in conditions which result in a risk that does need to be dealt may be reflected in the identification of "new" risks (re-identified).
Research	These risks require in-depth investigation to determine the root causes; some potential strategies require investigation to determine what benefit will be gained. For example, a risk on real-time performance may require some investigation into the proposed compiler and platform to determine the exact parameters. A bus- loading risk may require prototyping of one or more alternative architectures to determine which one will address the issue. These risks require **research**, and upon completion of the research, the risk is reassessed, based upon the additional information by repeating the review and assign step of the action planning process.
Eliminate	Risks that can be **eliminated** should be. This judgment is generally based upon the cost of eliminating the risk versus the costs of potential impact and the likelihood that it will occur. Risks that are eliminated are closed when the strategies to eliminate them are complete. Continuous risk identification will identify the risk again as a new risk should conditions change such that the strategies taken are no longer effective. Early identification and elimination of unnecessarily risky areas is a means of preventing risks.
Reduce	Risk exposure is a measure of the impact of a risk on the program and the likelihood or probability that it will occur. In **reducing** the risk exposure one can reduce either one or both of these factors. For example, given a risk that a piece of equipment will not be available on time, one could select a backup piece of equipment to use if the delivery does not occur. This may not be an ideal solution, and may still impact the schedule, but the overall potential effect on the program is reduced.

Table 7: Strategy Descriptions

The general question to ask and answer, is "What set of strategies best manages the program's risks?" A single strategy may resolve many risks, or may cause conflicts with other strategies. The best solution for any given risk is not necessarily the best answer for the program. Each program must identify a set of criteria by which strategies are evaluated. These criteria can include budget, personnel, schedule, product quality, specific components (e.g., the compiler must be delivered first), return on investment, and others. Good strategies, then, are those which meet the selection criteria. As with the evaluation of a single risk, matrices or trees can be constructed to view a set of strategies relative to the criteria, for example:

- dependency trees show the dependencies between risks, and therefore, identify those risks or conditions leading to those risks, which, if eliminated or greatly reduced, can have the same beneficial effect on several risks. Strategies for these root causes should be emphasized.

- dependency/interaction matrices identify the interactions between strategies and highlight conflicts (minimize these) and synergy (maximize this).
- cost/benefit matrices help correlate required resources and predicted gains.
- schedule and dependency matrices highlight which strategies need to be taken first.
- strategy vs. program area matrices identify areas of the program which may need additional budget reallocation.

The key to any of these types of matrices or relation diagrams is to provide information to support informed decisions. For a large set of risks, or complicated, interrelated strategies, it is vital that the relationships between risks and their potential strategies be understood before resources are committed. As new risks are identified and planning begun, their relationships to existing risks and strategies must also be understood to avoid unnecessary duplication of effort or negation of actions already taken.

One aspect of the cost of managing a risk is the cost of tracking it. For risks that will need to be tracked, the triggers to look for, how often status should be reported (as well as by whom and in what format), and how the tracking data is to be collected (automatically, manually derived from other data, etc.) must be identified. The cost of the tracking effort needs to be included in the cost of a strategy. The decision to require detailed, automated tracking of a risk should not be made without first understanding whether it is possible and its total cost. There may be alternative means of tracking a risk and of tracking the progress of mitigation strategies.

Decide on a strategy. During the process of evaluation, alternatives are eliminated that don't meet the selection criteria. This is documented along with the other risk information to capture complete information on each risk (conditions and criteria do change with time). The final decision is made based on the overall cost and benefit of the strategies to the program. These decisions are documented as any other program decision and this information is a part of the data retained for each risk. The strategies that are selected will generally require the development of a detailed task plan, schedule, WBS, and other normal types of program management information. The strategies for risk management then become tasks within the program.

Implement. The next phase of the paradigm, tracking, begins when action plans are implemented. Tracking is also used for those risks with contingency plans, to alert management to the need for implementing those contingency plans. Risks are tracked according to plan to provide visibility into the current state of the risks. Strategies are tracked and statused as any other task within the program. Risk action plans, like the risks themselves, need to be managed to ensure the plans are implemented and effective. Some level of authority, or multiple levels of authority, is needed to ensure proper review of plans for effective use of resources.

The plans developed during the action planning process form the basis for tracking and control processes of team risk management. The next section discusses risk tracking and control.

4.1.4 Tracking and Control

The risk tracking and control processes involve establishing and maintaining risk status information, defining action plans, and taking action based upon the status information. The essential elements of risk tracking and control are very similar to the equivalent processes in traditional program or project management and can be readily integrated into a program's established tracking and control processes and methods.

Tracking

The goal of risk tracking is to provide accurate and timely information to enable risk management and help prevent risks from adversely affecting the program by anticipating events, rather than reacting to them. This proactive character of risk management is achieved by establishing and maintaining risk metrics, indicators, and triggers that are "leading" indicators – those that provide insight into the nature of and potential for future events; and by presenting the resulting information to program decision makers in a timely and comprehensive way. The following are the three categories of information employed in risk tracking:

- ***Metrics*** are measures (qualitative and quantitative) of the important aspects of risks, as risks may impact the program. They are used for the individual and collective tracking of risks.
- ***Status indicators*** are used as a representation of the status of key elements of the program and include individual metrics or combinations of metrics. They are used to characterize a change in the status of risks.
- ***Triggers*** are the values of risk metrics or status indicators that reflect a significant change or event occurring within a program. They are used to report changes in the status of risks.

The specific risk metrics, status indicators, and triggers required for risk tracking vary from program to program and from risk to risk but fundamentally the choice for a particular program or risk is based upon the value of the content of the information. The criteria for their selection involves considerations of how effectively these measures convey a sense of the program's evolution, identify where and when the risk environment is changing, and identify where a situation may require a control decision.

Each risk being tracked has an update cycle and associated schedule for these updates. Typically, status is updated at least monthly, but particular risks may require a more frequent update, particularly when the program is entering a critical phase. These updates ensure that the data reported is current and accurate.

A summary presentation of metrics, status indicators, and triggers consolidates information from many sources throughout the program into a manageable number of indications. A representative example summary sheet is shown in Figure 4-11. The information provided by a summary presentation is a concise statement of the key information on risks that enables program decision makers to make timely and informed decisions regarding risk planning and actions.

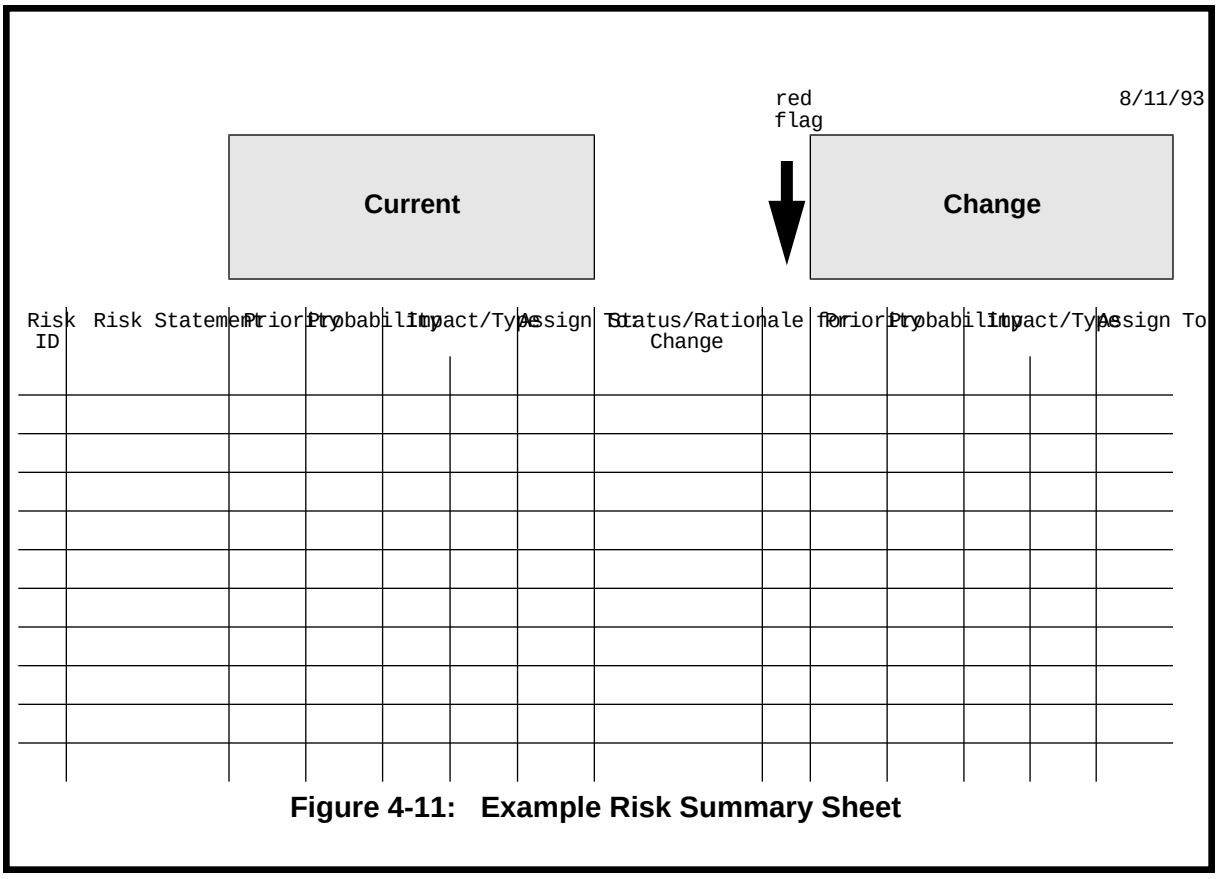


Figure 4-11: Example Risk Summary Sheet

Since each program has its own set of needs for risk-tracking metrics and status indicators, adding risk tracking involves selecting from a set of recommended methods, those that best fit a program's needs and that most effectively integrate into the program's existing tracking measures and processes. These tailored risk management processes provide a customized risk tracking and control environment for the program.

Control

Risk control focuses on actions to ensure that the program executes according to plan by reducing the potential for risks and controlling their adverse effects, before risks have significantly disrupted program activities. The plan for and the execution of actions are based on the analysis of the risk status indicators, metrics, and associated triggers. Specific risk control methods provide guidance on how to use risk-tracking information to determine the best course of action. These risk-control efforts are based upon the action plans developed as part of the routine team risk management action planning process. An important element in the implementation process is the close correlation that is needed between action planning, tracking, and control processes. Fundamentally, tracking and control provide the processes and the data required to execute and monitor plans and to make decisions regarding the direction of the program and the need for replanning in order to successfully meet program objectives.

While the details of the implementation of tracking and control within a program vary based upon the needs and specific characteristics of that program, the processes are integrated into routine program management activities. This integration into a program's routine activities is fundamental to the effective practice of all of the team risk management processes.

4.2 Baseline Risk Assessment

This section presents an overview of the baseline risk assessment, the activity that initiates the team risk management Process as shown previously in Figure 4-1, The Team Risk Management Process Set. Continuous risk management is a continual cycle of identifying and resolving program risks. The baseline risk assessment activity is a way to begin this cycle.

In a baseline risk assessment, a variety of methods and tools (see Table 8) are used to initially identify and analyze a set of risks and produce the initial Master Lists of Risks, one for the government and one for the contractor.

Paradigm	Methods/Tools	Communication Characteristics
Identify	• Group interview • Taxonomy-based questionnaire	• non-judgmental • non-attribution • confidential • peer grouping
Analyze	• Criteria filtering • Individual Top 5 • Nominal group technique • Comparison risk ranking	• individual voice • mutual understanding • consensus

Table 8: Baseline Risk Assessment Paradigm Methods, Tools, and Communication Characteristics

The basic steps involved in the baseline risk assessment process are shown in Figure 4-12. All of the baseline risk assessment activities are conducted by a trained risk assessment team. This assessment team may be part of the program's parent organization or may be independent of the organization. If the assessment team comes from the parent organization, it should be external to the program being assessed. Regardless of the team's composition, training is important to effectively carry out the risk assessment process.

The initial process step in a baseline risk assessment, **initiate**, involves establishing a commitment on the part of the organization's personnel to the team risk management process. The commitment involves the participation of personnel throughout the program and provides an overview of the process to all of the participants involved and prepares them for their roles in that process. This presentation is the start of the "buy-in" that is so important to introducing change into an organization.

Identification and a preliminary analysis of risks on the program are conducted in the **investigate** process step. A variety of methods can be employed, but generally the method used involves a group interview approach for risk identification and individual analysis of the risks. For

the interview a taxonomy-based questionnaire [Carr 93] and a non-judgmental, non-attribution group interview technique are employed and personnel from the program, participants, are interviewed in peer groups. The risk analysis activity involves the individual assessment of the impact, likelihood, and time frame (part of the criteria filtering method) associated with each risk identified in the interview process. In addition, a selection of the five most important risks to the program is made by each participant (Individual Top 5 method). Regardless of the specific method employed, these processes are the initial identification and analysis steps of the risk management process and the resulting information is used to facilitate management decisions on risks to the program.

The **consolidate** process step merges the risk data into a consistent package to prepare for the establishment of program priorities for the identified risks. This process involves the compilation of identification and analysis information on each risk and organization of this data. The result of this activity is the Master List of Risks for the program and a baseline data set for each risk. This information is the foundation for management's initial decision making and subsequent program planning activities for risks.

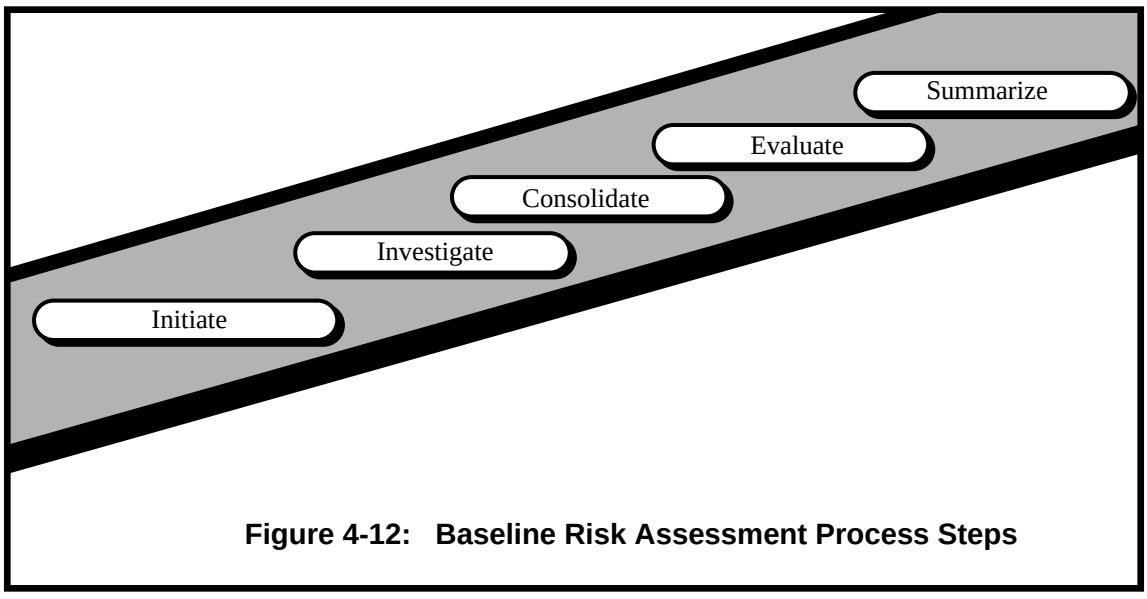


Figure 4-12: Baseline Risk Assessment Process Steps

The **evaluate** process step consists of activities where management becomes directly involved in the process by reviewing and prioritizing the most important risks on the program, known as Top N. This step is the mechanism to focus quickly on the most important risks and place them in a management-defined priority order. The methods employed in this step (such as the nominal group technique and comparison risk ranking) are designed using risk management principles and, in particular, incorporate methods that facilitate and enable a shared product vision, open communication, the expression of individual perception, and a systems perspective.

The final step in the baseline risk assessment is a presentation of the results, without attribution to any group or individual. This **summarize** step generally is conducted as a formal pre-

sentation to all program personnel who participated in the assessment process. It is at the end of this presentation that the results are formally delivered directly to the program manager, with the awareness that the program manager “owns” the results. While this step is the conclusion of the baseline risk assessment, this step initiates the continuous processes of team risk management.

Each partner—government and contractor—conducts a baseline risk assessment to define the risks that are associated with their respective organizations. The product of each of the baseline risk assessments is a Master List of Risks. There are two Master Lists, one for each partner organization, government or contractor, and each contains the prioritized Top N risks for the partner organization as well as all of the other identified risks organized into the four analysis bins (see Figure 4-13).

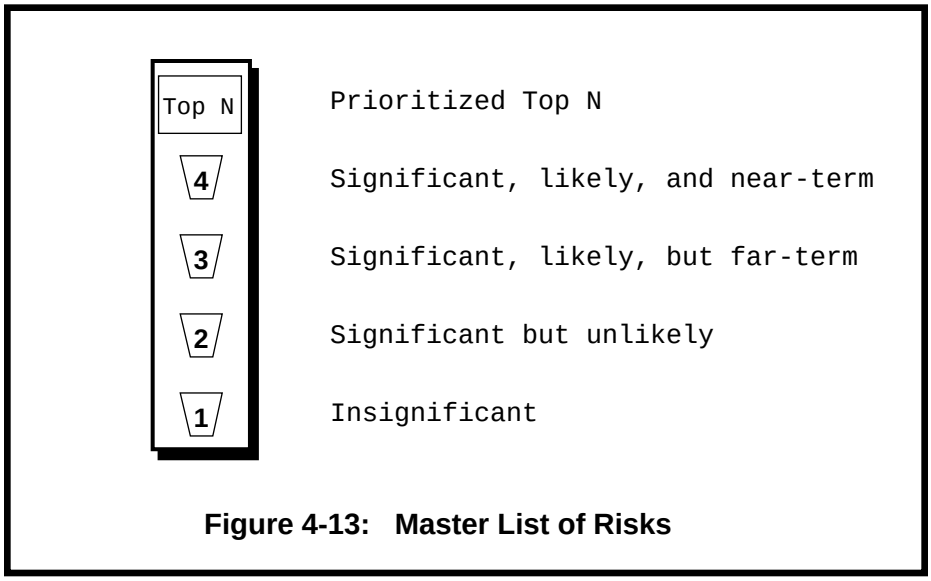


Figure 4-13: Master List of Risks

The Master Lists of Risks feed forward into the continuous loop of the team risk management process (see Figure 4-14) and serve as a reference point for the current risks in the program. All the risks on the Master List from each partner organization are input into the action planning process and a subset of the Top N risks are input into the initial team review process.

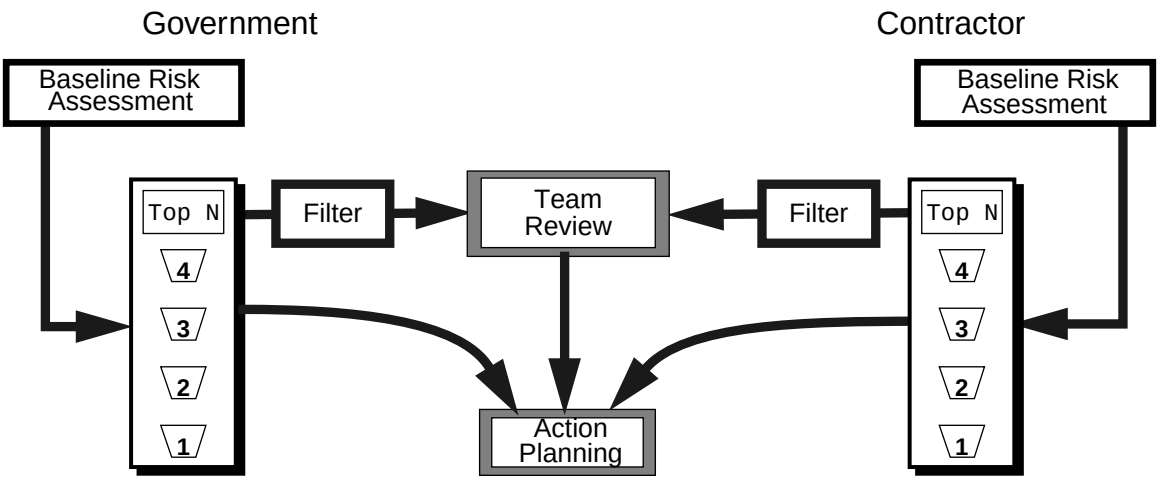


Figure 4-14: Outcome of Baseline Risk Assessment Results

4.3 Closure

Team risk management processes are founded upon the nine principles summarized in

Table 9 and empower organizations to cooperatively manage program risks. The approach is built upon a shared vision for success and combines the SEI risk management paradigm with a broad program-wide, inter-organizational, and intra-organizational team perspective.

• Shared product vision	• Value of Individual perception	• Proactive strategies
• Forward-looking search for uncertainties	• Systems perspective	• Systematic and adaptable methodology
• Open communications	• Integration into program management	• Routine and continuous processes

Table 9: Team Risk Management Principles

The processes and principles of team risk management are embodied in the methods and tools shown in Figure 4-15. With the shared product vision of team risk management providing the focus for program success, team risk management practices bring the government, contractor, and personnel throughout the program together in cooperative and proactive risk management.

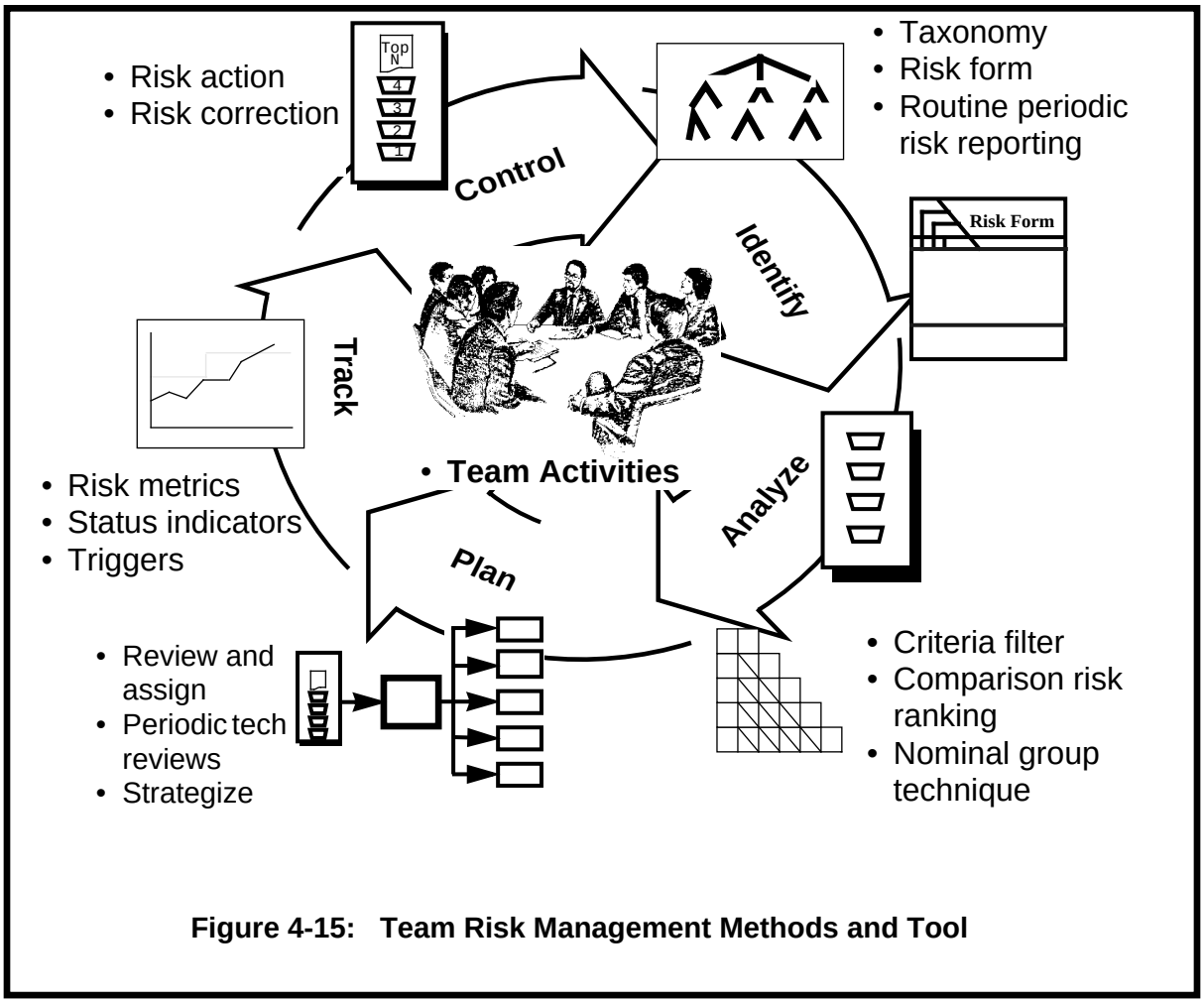


Figure 4-15: Team Risk Management Methods and Tool

5 Team Building and Communications

Successful teams are characterized by effective communications between all team members. Risks, problems, and crises often occur when communications break down in an organization. Communication underlies successful team risk management and is the foundation for team building between and within partner organizations.

Consider the scope of the communication and team-building challenges in a government program as reflected in Figure 5-1, which shows the communication lines between a government program management office and external agencies. Information about potential risks to the program can come from any of the communication lines as well as from within the program management office itself. Some of the lines of communication can be partially or totally blocked or have enormous time delays. The challenge is to find ways to open the communication pathways to the decision makers and speed up the synthesis of concerns and issues into actionable risks.

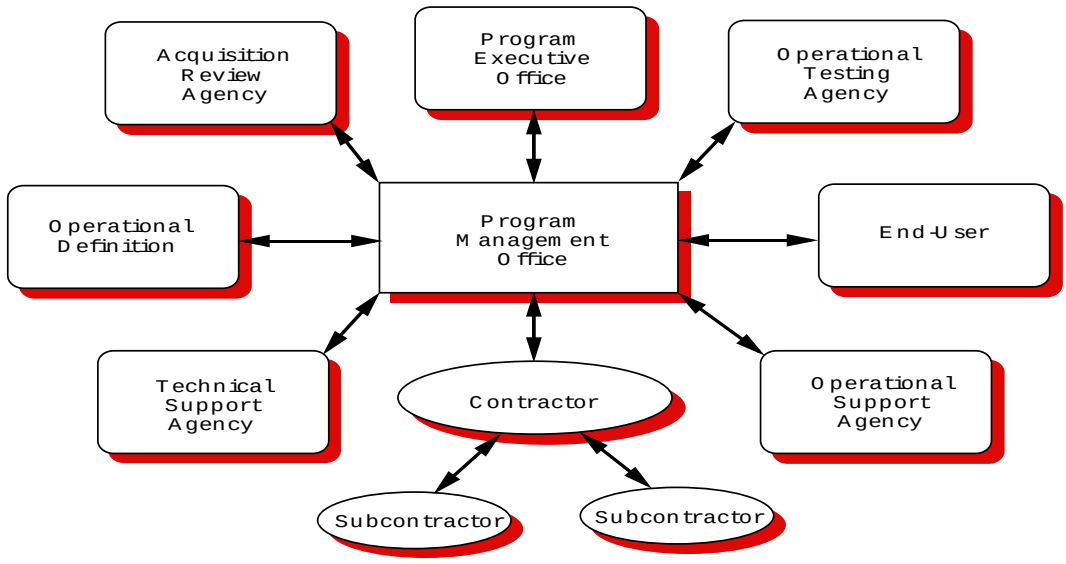


Figure 5-1: Communication Lines Between Government PMO and External Agencies

There are many reasons why risks are not communicated efficiently in a program. For example, the person who has an issue or concern with regard to their technical area may not have the program experience to understand all its implications, or how seriously the underlying risk could impact the program. Or they may assume that their concern is unlikely to turn into a problem because no one else is talking about it, concluding that “Everything will be OK,” or, “We’ll figure out a solution to that when we get there.” In software-dependent programs, those who understand the software risks may not have the expertise or communication path to rec-

ommend changes in the larger system (in the hardware, or in the aircraft itself, for example) that would mitigate risk most cost-effectively for the whole program.

While management has the primary authority and power to make changes and decide the course of the program, improving and maintaining an effective team is the responsibility of all of the members of the team. Management can communicate to the entire program that it is vital that risks be identified and communicated upward for resolution; can aggressively support those processes; can encourage team building and improved risk communication by fostering small inter-disciplinary groups to deal with risks as they are identified; can make risk communication and public support of it one of the points covered in the performance appraisals; and can publicize what is being done in risk planning, tracking, and control for identified risks. Through these and similar efforts, management can provide leadership in achieving effective communication and strong, interpersonal, team cooperation.

Team members must allow and encourage management to behave in new ways, by responding quickly to requests and in general fostering continuing change by not immediately interpreting any lapse into “old ways” as a sign that the risk management effort has come to an end. Specifically, program staff members must understand and accept risk management practices as worthwhile and permanent, even if they represent a significant change from the way the organization has operated in the past. However, the responsibility of realizing that shared vision and of creating a sense of collective ownership and responsibility requires all team members to contribute actively to the communications and teambuilding efforts.

6 Observations and Summary

There are many challenges when applying the team risk management process within an organization, but the central issue is one of establishing a team-oriented environment characterized by a risk ethic [Kirkpatrick 92]. Toward this end, the Risk Program within the SEI has been maturing its risk management methods by applying the methods to government and industry software-dependent development programs.

While most managers feel that they are managing risks [Kirkpatrick 92] and that successful managers are generally good risk managers [Boehm 91], the preliminary results of the SEI's Risk Program demonstrate that few organizations have explicit policies for risk management; further, most organizations that have addressed risk issues have done so through undocumented or ad hoc policies [Kirkpatrick 92].

Software risks are among the least measured or managed risks in a system; yet, in technology areas more familiar to most Department of Defense program managers (e.g. aerodynamics, propulsion, air frames), the risks are well managed. Generally, managers are effective in managing the risks associated with the technologies they know and consequently overall risk management activity is very dependent on individual judgment and experience [Kirkpatrick 92].

During the field testing and implementation of team risk management, the introduction of a structured process for identifying, analyzing, and generally managing software technical risks has altered the perception of risks within an organization and expanded the awareness of these issues. Even in the programs where "problem" management was used as a risk management vehicle, the incorporation of the structured, depersonalized team risk management process, coupled with the proactive planning strategies, has enhanced the program's risk management capabilities.

In the continuing application of the risk management process to large software development programs, the most dramatic effect has been in opening the communication channels for dialogues within organizations relating to risks and risk management. The non-attribution which exists throughout all steps of the process has proven extremely effective in fostering openness in risk discussion. This effect has been observed in peer group interactions as well as in joint management sessions.

The impact of the application of team risk management and the basic risk management process to government and industry organizations is evidenced in the evaluations and comments provided by organizations participating in the testing of the methods. A sample of the comments include:

"brought out many risks that had not been previously identified"
"opportunity to consider some areas... not focused on before"
"comfortable setting to express concerns"
"catalyst to open communications"
"process broke down feelings and barriers that existed"
"comprehensive"

Through team risk management practices, program personnel are empowered with methods and tools that capitalize on the characteristic that, collectively, teams (working together based upon the nine principles of team risk management) actually possess more knowledge, think in a greater variety of ways, and are more effective than the totality of the team members working as individuals. Institutionalizing the team risk management approach and enabling organizations to realize self-sufficiency in risk management is the major challenge and objective of the SEI's Team Risk Management Project.

7 Acknowledgments

We would like to thank the Navy PEO(A) for sponsoring this work. Without this support, these efforts would not have continued. We especially thank Captain David Nordean, whose ideas and gentle prodding spurred us on when the going got tough.

References

[Boehm 91] Boehm, Barry W. “Software Risk Management: Principles and Practices.” *IEEE Software* 8, 1 (January 1991): 32-41.

[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.

[Dorofee 93] Dorofee, Audrey. “Team Risk Management: A New Paradigm.” Paper presented at the Software Engineering Symposium, Pittsburgh, Pa., August 23-26, 1993.

[FitzGerald 90] FitzGerald, Jerry; & FitzGerald, Ardra F. “A Methodology for Conducting a Risk Assessment.” *Designing Controls into Computerized Systems.* 2nd ed., Redwood City, Ca.: Jerry FitzGerald & Associates, 1990.

[Higuera 93] Higuera, Ronald P.; & Gluch, David P. “Risk Management and Quality in Software Development.” Paper presented at the Eleventh Annual Pacific Northwest Software Quality Conference, Portland, Oregon, October 18-20, 1993.

[Kirkpatrick 92] Kirkpatrick, Robert J.; Walker, Julie A.; & Firth, Robert. *Software Development Risk Management: An SEI Appraisal* (SEI Technical Review ‘92). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1992.

[Scholtes 88] Scholtes, Peter R. *The Team Handbook: How to Use Teams to Improve Quality.* Joiner Associates, Inc., 1988.

[SEI 92] Software Engineering Institute. “The SEI Approach to Managing Software Technical Risks.”*Bridge*, October 1992:19-21.

[SEI 93] Software Engineering Institute. “Team Risk Management in Software-Dependent Development Programs.” SEI draft report, 1993.

[Xerox 92] Xerox Corporation/Carnegie Mellon University. *Problem-Solving Process User’s Manual*. Xerox Corporation/Corporate Education and Training, Stamford, Conn., 1992.

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS
None

2a. SECURITY CLASSIFICATION AUTHORITY
N/A

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for Public Release
Distribution Unlimited

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
N/A

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
CMU/SEI-94-SR-1

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Software Engineering Institute

6b. OFFICE SYMBOL (if applicable)
SEI

7a. NAME OF MONITORING ORGANIZATION
SEI Joint Program Office

6c. ADDRESS (city, state, and zip code)
Carnegie Mellon University
Pittsburgh PA 15213

7b. ADDRESS (city, state, and zip code)
HQ ESC/ENS
5 Eglin Street
Hanscom AFB, MA 01731-2116

8a. NAME OFFUNDING/SPONSORING ORGANIZATION
SEI Joint Program Office

8b. OFFICE SYMBOL (if applicable)
ESC/ENS

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
F1962890C0003

8c. ADDRESS (city, state, and zip code))
Carnegie Mellon University
Pittsburgh PA 15213

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO	PROJECT NO.	TASK NO	WORK UNIT NO.
63756E	N/A	N/A	N/A

11. TITLE (Include Security Classification)
An Introduction to Team Risk Management (Version 1.0)

12. PERSONAL AUTHOR(S)
Ronald P. Higuera, David P. Gluch, Audrey J. Dorofee, Richard L. Murphy, Julie A. Walker, Ray C. Williams

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (year, month, day)	15. PAGE COUNT
Final	FROM TO	May 1994	56

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (continue on reverse of necessary and identify by block number)
FIELD	GROUP	SUB. GR.	

19. ABSTRACT (continue on reverse if necessary and identify by block number)

(Version 1.0) Team Risk Management defines the organizational structure and operational activities for managing risks throughout all phases of the life-cycle of a software-dependent development program such that all individuals within the organizations, groups, departments, and agencies directly involved in the program are participating team members. Through the adoption of team risk management, the government and contractor are provided with processes, methods, and tools that enable both organizations, individually and jointly, to be increasingly anticipatory in decision-making processes. This report introduces the team risk management approach for managing risks within a software-dependent development program.

(please turn over)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ■ SAME AS RPT □ DTIC USERS ■

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified, Unlimited Distribution

22a. NAME OF RESPONSIBLE INDIVIDUAL
Thomas R. Miller, Lt Col, USAF

22b. TELEPHONE NUMBER (include area code)
(412) 268-7631

22c. OFFICE SYMBOL
ESC/ENS (SEI)

ABSTRACT — continued from page one, block 19