U.S. Department of Energy

Office of Management, Budget and Evaluation

Risk Management

Initiated by: Office of Engineering and Construction Management

RISK MANAGEMENT

Risk has always been a concern in the acquisition of DOE capital assets. The acquisition process itself is designed, to a large degree, to allow risks to be controlled from conception to delivery of a system. Unfortunately, in the past, some project directors (PDs), project managers (PMs), and decision-makers have viewed risk as something to be avoided. Any project that involved risk was subject to intense review and oversight. This attitude has changed. DOE managers recognize that risk is inherent in any project and that it is necessary to analyze future project events to identify potential risks and take measures to handle them.

Risk management is concerned with the outcome of future events, whose exact outcome is unknown, and the development of strategies to deal with these uncertainties, over a range of possible outcomes. In general, outcomes are categorized as favorable or unfavorable, and risk management is the art and science of planning, assessing, and handling future events to ensure favorable outcomes. The alternative to risk management is crisis management, a resource-intensive process that is normally constrained by a restricted set of available options.

1.0 PURPOSE AND SCOPE

This Practice is designed to provide acquisition professionals and program and project management offices with a reference for dealing with system acquisition risks. It is intended to be useful as an aid in classroom instruction and as a reference for practical applications. Much of the material in this Practice is derived from the Department of Defense, *Defense Acquisition Deskbook.*

1.2 Organization of the Practice

This Practice discusses risk and risk management, defines terms, and introduces basic risk management concepts (Section 4).

Section 5 examines risk management concepts relative to the Federal acquisition process, and illustrates how risk management is an integral part of program management, describes interaction with other acquisition processes, and identifies and discusses the various types of acquisition risks.

Section 6 discusses the implementation of a risk management program from the perspective of a PD/PM, and focuses on practical application issues such as risk management program design options, project management risk management organizations, and criteria for a Risk Management Information System.

Section 7, the final section, describes a number of techniques that address the aspects (phases) of risk management, i.e., planning, assessment, handling, and monitoring.

This Practice also contains an Appendix that is intended to provide reference material and examples, in addition to backup detail for some of the concepts presented in the main portion of the Practice.

This Practice is a source of background information and provides a starting point for a risk management program. None of the material is mandatory. PDs/PMs should tailor the approaches and techniques to fit their needs.

2.0 APPROACH TO RISK MANAGEMENT

This Practice emphasizes a risk management approach that is disciplined, forward-looking, and continuous.

In 1986, the Government Accounting Office (GAO) developed a set of criteria as an approach to good risk assessments. These criteria, with slight modification, apply to all aspects of risk management and are encompassed in the Practice's approach. They are:

- *Planned Procedures*. Risk management is planned and systematic.
- *Prospective Assessment*. Potential future problems are also considered, not just current problems.
- *Attention to Technical Risk*. There is explicit attention to technical risk.
- *Documentation*. All aspects of the risk management program are recorded and the data maintained.
- *Continual Process*. Risk assessments are made throughout the acquisition process; handling activities are continually evaluated and changed if necessary; and critical risk areas are always monitored.

While these criteria are not solely sufficient to determine the "health" of a program, they are important indicators of how well a risk management process is being implemented. A proactive risk management process is a good start toward a successful risk management program.

3.0 RISK AND RISK MANAGEMENT

This section introduces the concepts of risk and risk management by explaining risk-related definitions and by identifying the characteristics of acquisition risks. It also presents and discusses a structured concept for risk management and its five subordinate processes.

3.1 Overview

The Federal risk management concept is based on the principle that risk management must be forward-looking, structured, informative, and continuous. The key to successful risk management is early recognition, planning, and aggressive execution. Good planning ensures an organized, comprehensive, and iterative approach for identifying and assessing the risk and handling options necessary to refine a project's acquisition strategy. To support these efforts, assessments should be performed as early as possible in the life cycle to ensure that critical technical, schedule, and cost risks are addressed with mitigating actions incorporated into planning and budget projections.

PDs/PMs should frequently update project risk assessments and tailor management strategies accordingly. Early information provides data that helps when writing a Request for Proposal and assists in Source Selection planning. As a project progresses, new information improves insight into risk areas which allows the development of effective risk handling strategies. The net result promotes executable projects.

Effective risk management requires involvement of the entire project team and also requires help from outside experts knowledgeable in critical risk areas (e.g., threat, technology, design, manufacturing, logistics, schedule, and cost). In addition, the risk management process should cover hardware, software, the human element, and integration issues. Outside experts may include representatives from the user, laboratories, contract management, test, logistics, sustainment communities, and industry. Users, essential participants in trade analyses, should be part of the assessment process so that an acceptable balance among cost, schedule, performance, and risk can be reached. A close relationship between the Government and industry, and later with the selected contractor(s), promotes an understanding of project risks and assists in developing and executing the management efforts.

Successful risk management programs generally have the following characteristics:

- Feasible, stable, and well-understood user requirements
- A close relationship with user, industry, and other appropriate participants
- A planned and structured risk management process, integral to the acquisition process
- An acquisition strategy consistent with risk level and risk-handling strategies
- Continual reassessment of project and associated risks
- A defined set of success criteria for all cost, schedule, and performance elements, e.g., Performance Baseline (PB) thresholds
- Metrics to monitor effectiveness of risk-handling strategies
- Effective Test and Evaluation Program
- Formal documentation.

PDs/PMs should follow the guidelines below to ensure that a risk management program possesses the above characteristics.

- Assess project risks, using a structured process, and develop strategies to manage these risks throughout each acquisition phase.
- Identify early and intensively manage those design parameters that critically affect cost, capability, or readiness.
- Use technology demonstrations/modeling/simulation and aggressive prototyping to reduce risks.
- Use test and evaluation as a means of quantifying the results of the risk-handling process.
- Include industry and user participation in risk management.
- Use research and development, testing, and evaluation, as well as early operational assessments when appropriate.
- Establish a series of “risk assessment reviews” to evaluate the effectiveness of risk handling against clearly defined success criteria.
- Establish the means and format to communicate risk information and to train participants in risk management.
- Prepare an assessment training package for project personnel and others, as needed.
- Acquire approval of accepted risks at the appropriate decision level.

In general, management of software risk is the same as management of other types of risk and techniques that apply to hardware programs are equally applicable to software intensive programs. However, some characteristics of software make this type of risk management different, primarily because it is difficult to:

- Identify software risk.
- Estimate the time and resources required to develop new software, resulting in potential risks in cost and schedule.
- Test software completely because of the number of paths that can be followed in the logic of the software.
- Develop new programs because of the rapid changes in information technology and an ever-increasing demand for quality software personnel.

3.2 Risk Management Structure and Definitions

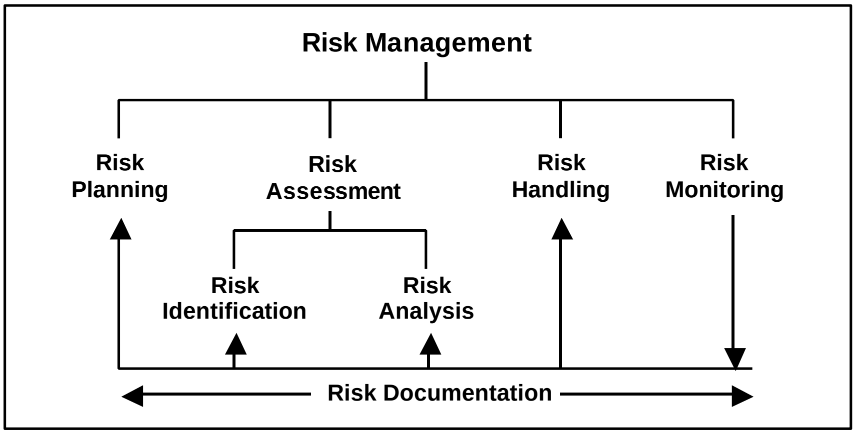


Figure 1. Risk Management Structure

Although each risk management strategy depends upon the nature of the system being developed, research reveals that good strategies contain the basic processes and structure shown in Figure 1. This structure is sometimes also referred to as the Risk Management Process Model. The application of these processes varies with acquisition phases and the degree of system definition; all should be integrated into the project management function. The elements of the structure are discussed in the following paragraphs. Definitions for the processes and elements of risk management are provided as follows:

Risk is a measure of the potential inability to achieve overall project objectives within defined cost, schedule, and technical constraints. It has two components: (1) the probability/likelihood of failing to achieve a particular outcome, and (2) the consequences/impacts of failing to achieve that outcome.

Risk events are elements of an acquisition that should be assessed to determine the level of risk, i.e., things that could go wrong in a project. The events should be defined to a level where an individual can comprehend the potential impact and its causes. For example, a potential risk event for a turbine engine could involve a turbine blade vibration. Related to this vibration could be a series of potential risk events that should be selected, examined, and assessed by subject-matter experts.

The relationship between the two components of risk—probability and consequence/ impact—is complex. To avoid obscuring the results of an assessment, the risk associated with an event should be characterized in terms of its two components. As part of the assessment, there is also a need for backup documentation containing the supporting data and assessment rationale.

Risk management is the act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program.

Risk planning is the process of developing and documenting an organized, comprehensive, and interactive strategy and methods for identifying and tracking risk areas, developing risk-handling plans, performing continuous risk assessments to determine how risks have changed, and assigning adequate resources.

Risk assessment is the process of identifying and analyzing project areas and critical technical process risks to increase the probability/likelihood of meeting cost, schedule, and performance objectives. *Risk identification* is the process of examining the project areas and each critical technical process to identify and document the associated risk.

Risk analysis is the process of examining each identified risk area or process to refine the description of the risk, isolating the cause, and determining the effects. It includes risk rating and prioritization in which risk events are defined in terms of their probability of occurrence, severity of consequence/impact, and relationship to other risk areas or processes.

Risk handling is the process that identifies, evaluates, selects, and implements options in order to set risk at acceptable levels given project constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, and the associated cost and schedule. The most appropriate strategy is selected from these handling options. For purposes of this Practice, risk handling is an all-encompassing term whereas risk mitigation is one subset of risk handling.

Risk monitoring is the process that systematically tracks and evaluates the performance of risk-handling actions against established metrics throughout the acquisition process and develops further risk-handling options, as appropriate. It feeds information back to the other risk management activities of planning, assessment, and handling as shown in Figure 1.

Risk documentation is recording, maintaining, and reporting assessments, handling analysis and plans, and monitoring results. It includes all plans, reports for the PD/PM and decision authorities, and reporting forms that may be internal to the PD/PM.

3.3 Risk Discussion

Implicit in the definition of risk is the concept that risks are future events, i.e., potential problems, and that there is uncertainty associated with the project if these risk events occur. Therefore, there is a need to determine, as much as possible, the probability of a risk event occurring and to estimate the consequence/impact if it occurs. The combination of these two factors determines the level of risk. For example, an event with a low probability of occurring, yet with severe consequences/impacts, may be a candidate for handling. Conversely, an event with a high probability of happening, but the consequences/impacts of which do not affect a program, may be acceptable and require no handling.

To reduce uncertainty and apply the definition of risk to acquisition projects, PDs/PMs must be familiar with the types of acquisition risks, understand risk terminology, and know how to measure risk. These topics are addressed in the next several sections.

3.3.1 Characteristics of Acquisition Risk

Acquisition projects tend to have numerous, often interrelated, risks. They are not always obvious—relationships may be obscure, and they may exist at all project levels throughout the life of a project. Risks occur in the program (program plans, etc.); in support provided by other Government agencies; in threat assessment; and in prime contractor processes, engineering, manufacturing processes, and technology. The interrelationship among risk events may cause an increase in one due to the occurrence of another. For example, a slip in schedule for an early test event may adversely impact subsequent tests, assuming a fixed period of test time is available.

Another important risk characteristic is the time period before a risk future event occurs, because time is critical in determining risk-handling options. If an event is imminent, the PD/PM must resort to crisis management. An event that is far enough in the future to allow management actions may be controllable. The goal is to avoid the need to revert to crisis management and problem solving by proactive risk management.

An event's probability of occurrence and consequences/impacts may change as the development process proceeds and information becomes available. Therefore, throughout the development phase, PDs/PMs should reevaluate known risks on a periodic basis and examine the project for new risks.

3.3.2 Project Products, Processes, Risk Areas, and Risk Events

Project risk includes all risk events and their relationships to each other. It is a top-level assessment of impact to the project when all risk events at the lower levels of the project are considered. Project risk may be a roll-up of all low-level events; however, most likely, it is a subjective evaluation of the known risks by the PD/PM, based on the judgment and experience of experts. Any roll-up of project risks must be carefully done to prevent key risk issues from "slipping through the cracks." Identifying project risk is essential because it forces the PD/PM to consider relationships among all risks and may identify potential areas of concern that would have otherwise been overlooked. One of the greatest strengths of a formal, continuous risk management process is the proactive quest to identify risk events for handling and the reduction of uncertainty that results from handling actions.

A project has continuous demands on its time and resources. It is, at best, difficult, and probably impossible, to assess every potential area and process. To manage risk, PDs/PMs should focus on the critical areas that could affect the outcome of their projects. Work Breakdown Structure (WBS) product and process elements and industrial engineering and manufacturing processes contain most of the significant risk events. Risk events are determined by examining each WBS element and process in terms of sources or areas of risk. Broadly speaking, these sources generally can be grouped as cost, schedule, and performance, with the latter including technical risk. Following are some typical risk areas:

- ***Threat.*** The sensitivity of the project to uncertainty in the threat description, the degree to which the system design would have to change if the threat's parameters change, or the vulnerability of the program to foreign intelligence collection efforts (sensitivity to threat countermeasure).
- ***Requirements.*** The sensitivity of the project to uncertainty in the system description and requirements except for those caused by threat uncertainty.
- ***Design.*** The ability of the system configuration to achieve the project's engineering objectives based on the available technology, design tools, design maturity, etc.
- ***Test and Evaluation.*** The adequacy and capability of the test and evaluation effort to assess attainment of significant performance specifications and determine whether the systems are operationally effective and suitable.
- ***Modeling and Simulation.*** The adequacy and capability of modeling and simulation to support all phases of a project using verified, valid, and accredited modeling and simulation tools.
- ***Technology.*** The degree to which the technology proposed for the project has been demonstrated as capable of meeting all of the project's objectives.
- ***Logistics.*** The ability of the system configuration to achieve the project's logistics objectives based on the system design, maintenance concept, support system design, and availability of support resources.
- ***Production.*** The ability of the system configuration to achieve the project's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources such as facilities and personnel.
- ***Concurrency.*** The sensitivity of the project to uncertainty resulting from the combining or overlapping of life cycle phases or activities.
- ***Capability of Developer.*** The ability of the developer to design, develop, and manufacture the system. The contractor should have the experience, resources, and knowledge to produce the system.
- ***Cost/Funding.*** The ability of the system to achieve the project's life cycle cost objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined).
- ***Management.*** The degree in which project plans and strategies exist and are realistic and consistent. The Government's acquisition team should be qualified and sufficiently staffed to manage the program.

- ***Schedule.*** The adequacy of the time allocated for performing the defined tasks, e.g., developmental, production, etc. This factor includes the effects of scheduling decisions, the inherent errors in the schedule estimating technique used, and external physical constraints.

Critical risk processes are the developer's engineering and production processes that, historically, have caused the most difficulty during the development and/or production phases of acquisition projects. These processes include, but are not limited to design, test, production, facilities, logistics, and management. These processes are included in the critical risk areas and are addressed separately to emphasize that they focus on processes. See Figure 2 for an example of the template for product development. The templates are the result of a Defense Science Board task force, composed of Government and industry experts, who identified engineering processes and control methods to minimize risk in both Government and industry. The task force defined these critical events in terms of the templates, which are briefly discussed later. Go to the following web site to obtain a copy of Department of Defense 4245.7-4: http://web7.whs.osd.mil/dodiss/publications/pub2.htm.

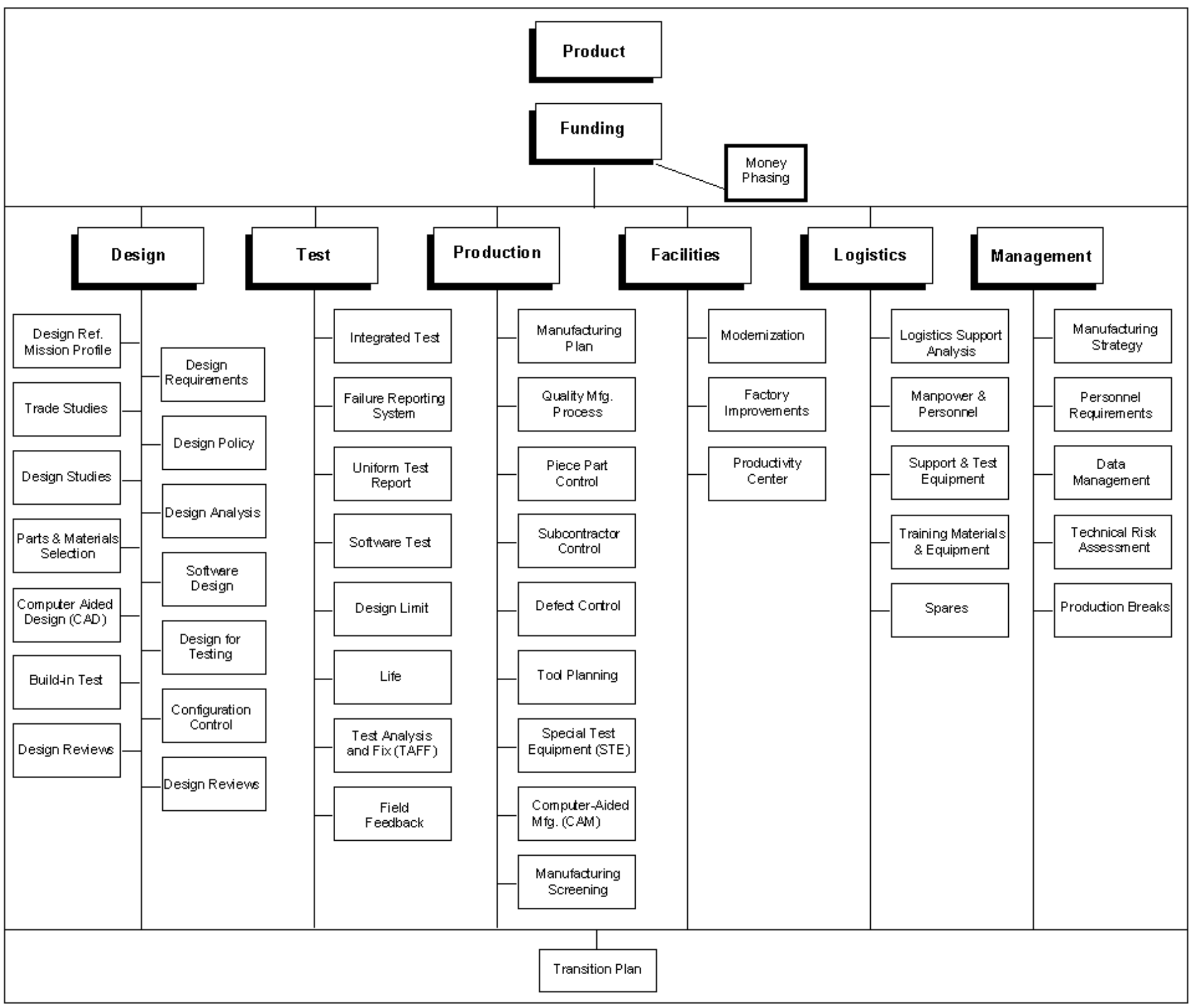


Figure 2. Critical Process Areas and Templates

Additional areas, such as manpower, environmental impact, systems safety and health, and systems engineering, that are analyzed during program plan development provide indicators for additional risk. The PD/PM should consider these areas for early assessment since failure to do so could cause dire consequences/impacts in the project's latter phases.

In addition, PDs/PMs should address the uncertainty associated with security—an area sometimes overlooked by developers. PDs/ PMs must recognize that, in the past, classified projects have experienced difficulty in access, facilities, clearances, and visitor control. Failure to manage these aspects of a classified project could adversely affect cost and schedule.

3.4 Risk Planning

3.4.1 Purpose of Risk Plans

Risk planning is the detailed formulation of a plan of action for the management of risk. It is the process to:

- Develop and document an organized, comprehensive, and interactive risk management strategy
- Determine the methods to be used to execute a PDs/PM's risk management strategy
- Plan for adequate resources.

Risk planning is iterative and includes describing and scheduling the activities and processes to assess (identify and analyze), handle, monitor, and document the risk associated with a project. The result is the Risk Management Plan (RMP).

3.4.2 Risk Planning Process

The PD/PM should periodically review the plan and revise it, if necessary. Some events such as: (1) a change in acquisition strategy, (2) preparation for a major decision point, (3) technical audits and reviews, and (4) an update of other project plans may drive the need to update an existing plan.

Planning begins by developing and documenting a risk management strategy. Early efforts establish the purpose and objective, assign responsibilities for specific areas, identify additional technical expertise needed, describe the assessment process and areas to consider, delineate procedures for consideration of handling options, define a risk rating scheme, dictate the reporting and documentation needs, and establish report requirements and monitoring metrics. This planning should also address evaluation of the capabilities of potential sources as well as early industry involvement.

The PD's/PM's strategy to manage risk provides the project team with direction and basis for planning. Initially formalized during a program's pre-acquisition phase and updated for each subsequent program phase, the strategy should be reflected in the project's acquisition strategy, which with requirement and threat documents, known risks, and system and project characteristics are sources of information for PD/PM use to devise a strategy and begin developing a RMP. Since the Government and contractor team's ability to develop and manufacture the system affects the project's risks, industry can provide valuable insight into this area of consideration.

The plan is the road map that tells the Government and contractor team how to get from where the project is today to where the PD/PM wants it to be in the future. The key to writing a good plan is to provide the necessary information so the integrated project team (IPT) knows the objectives, goals, and the PD's/PM's risk management process. Since it is a map, it may be specific in some areas, such as the assignment of responsibilities for Government and contractor participants and definitions, and general in other areas to allow users to choose the most efficient way to proceed. For example, a description of techniques that suggests several methods for evaluators to use to assess risk is appropriate, since every technique has advantages and disadvantages depending on the situation.

Appendix A contains two examples of a risk plan and a summary of the format is shown in Figure 3.

Introduction
Summary
Definitions
Risk Management Strategy and Approach
Organization
Risk Management Process and Procedures
Risk Planning
Risk Assessment
Risk Handling
Risk Monitoring
Risk Management Information System, Documentation, and Reports

Figure 3. A Risk Management Plan Outline/Format

In a decentralized project management risk management organization, the project's risk management coordinator may be responsible for risk management planning. See Sections 5.3, Risk Management Organization, and 6.2, Risk Planning Techniques.

3.5 Risk Assessment

3.5.1 Purpose of Risk Assessments

The primary objective of assessments is to identify and analyze project risks so that the most critical among them may be controlled. Assessments are factors that managers should consider in setting cost, schedule, and performance objectives because they provide an indication of the probability/likelihood of achieving the desired outcomes.

3.5.2 Risk Assessment Process

Risk assessment is the problem definition stage of management that identifies and analyzes (quantifies) prospective project events in terms of probability and consequences/impacts. The results form the basis for most risk management actions. It is probably the most difficult and time-consuming part of the management process. There are no quick answers or shortcuts. Tools are available to assist evaluators in assessing risk, but none are totally suitable for any project and may be highly misleading if the user does not understand how to apply them or interpret the results. Despite its complexity, risk assessment is one of the most important phases of the risk process because the caliber and quality of assessments determine the effectiveness of a management program.

The components of assessment, identification, and analysis are performed sequentially with identification being the first step.

Risk identification begins by compiling the project's risk events. PDs/PMs should examine and identify project events by reducing them to a level of detail that permits an evaluator to understand the significance of any risk and identify its causes, i.e., risk drivers. This is a practical way of addressing the large and diverse number of potential risks that often occur in acquisition projects. For example, a WBS level-4 or -5 element may generate several risk events associated with a specification or function, e.g., failure to meet turbine blade vibration requirements for an engine turbine design.

Risk events are best identified by examining each WBS product and process element in terms of the sources or areas of risk.

Risks are those events that evaluators (after examining scenarios, WBS, or processes) determine would adversely affect the project. Evaluators may initially rank events by probability and consequence/impact of occurrence before beginning analysis to focus on those most critical.

Risk analysis is a technical and systematic process to examine identified risks, isolate causes, determine the relationship to other risks, and express the impact in terms of probability and consequences/impacts.

In practice, the distinction between risk identification and risk analysis is often blurred because there is some risk analysis that occurs during the identification process. For example, if, in the process of interviewing an expert, a risk is identified, it is logical to pursue information on the probability of it occurring, the consequences/impacts, the time associated with the risk (i.e., when it might occur), and possible ways of dealing with it. The latter actions are part of risk analysis and risk handling, but often begin during risk identification.

Prioritization is the ranking of risk events to determine the order of importance. It serves as the basis for risk-handling actions. Prioritization is part of risk analysis.

IPTs typically perform risk assessments in a decentralized risk management organization as described in Section 5.3. If necessary, the team may be augmented by people from other program areas or outside experts. Section 6.2, Risk Assessment Techniques, elaborates on this for each of the described assessment techniques.

3.5.3 Timing of Risk Assessments

The assessment process begins during the last half of the Initiation phase and continues throughout the subsequent acquisition phases. The PD/PM should continually reassess the project at increasing levels of detail as the project progresses through the acquisition phases and more information becomes available. There are, however, times when events may require new assessments, i.e., a major change in the acquisition strategy.

3.5.4 Conducting Risk Assessments

There is no standard approach to assessing risk because methods vary according to the technique employed, the phase of the project, and the nature of the project itself; however, some top-level actions are typically common to all methods. They are grouped in Figure 4 into pre-risk assessment activities, risk identification activities, and risk analysis activities. Each risk category or area, e.g., cost, schedule, and performance, includes a core set of assessment tasks and is related to the other two categories. This relationship requires supportive analysis among areas to ensure the integration of the assessment process. For example, a technical assessment probably should include a cost and schedule analysis in determining the technical risk impact. The results of the assessments, normally conducted by IPTs follow:

Performance/Technical Assessment

- Provides technical foundation
- Identifies and describes project risks, i.e., threat, technology, design, manufacturing, etc.
- Prioritizes risks with relative or quantified weight for project impact
- Analyzes risks and relates them to other internal and external risks
- Quantifies associated project activities with both time duration and resources
- Quantifies inputs for schedule assessment and cost estimate
- Documents technical basis and risk definition for the risk assessment.

Schedule Assessment

- Evaluates baseline schedule inputs
- Incorporates technical assessment and schedule uncertainty inputs to project schedule model
- Evaluates impacts to project schedule based on technical team assessment

- Performs schedule analysis on project integrated master schedule
- Quantifies schedule excursions reflecting effects of cost risks, including resource constraints
- Provides Government schedule assessment for cost analysis and fiscal year planning
- Reflects technical foundation, activity definition, and inputs from technical and cost areas
- Documents schedule basis and risk impacts for the risk assessment.

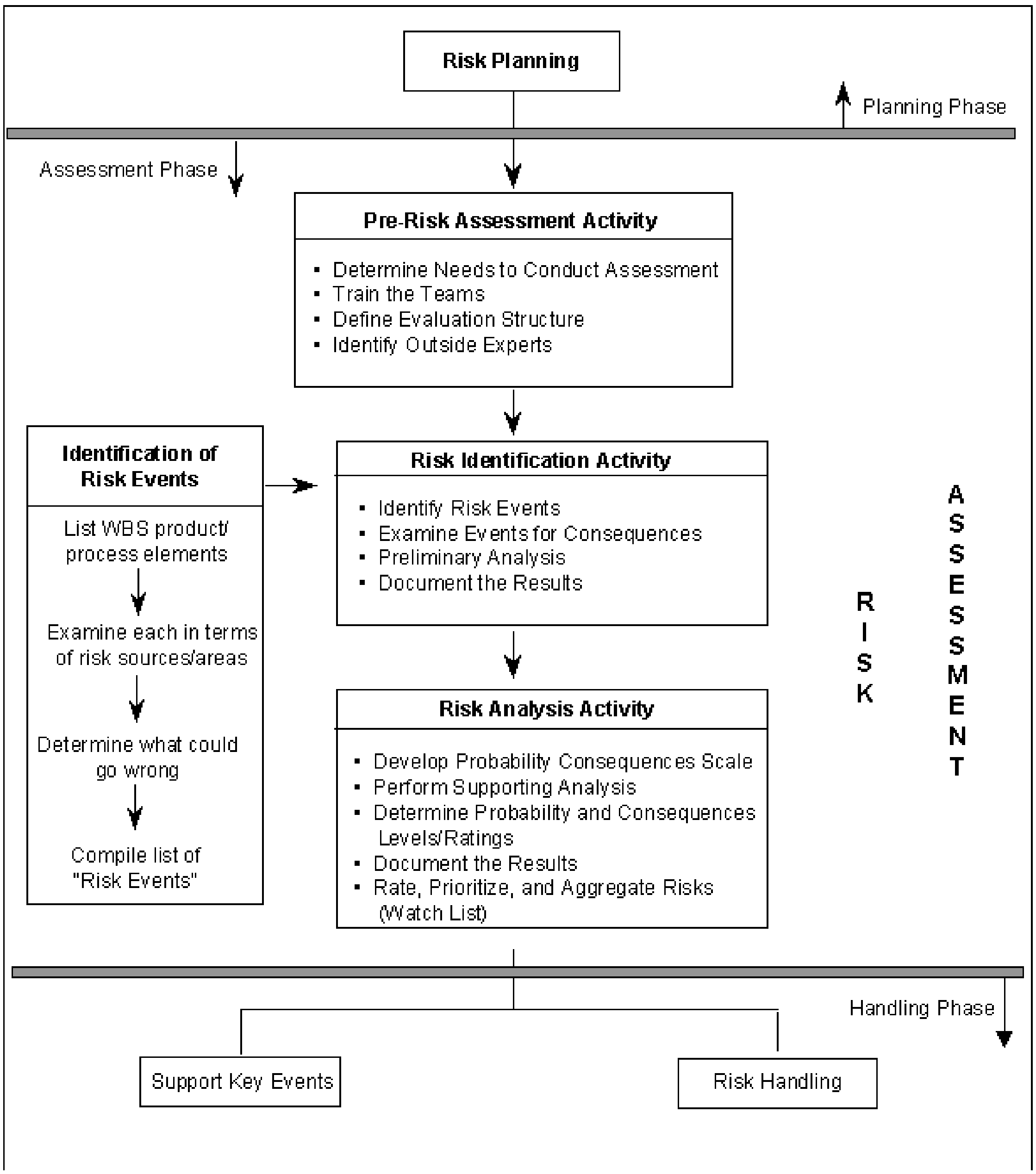


Figure 4. Risk Assessment

Cost Estimate and Assessment

- Builds on technical and schedule assessment results
- Translates technical and schedule risks into cost
- Derives cost estimate by integrating technical risk and schedule risk impacts with resources
- Establishes budgetary requirements consistent with fiscal year planning
- Determines if the phasing of funds supports technical and acquisition approach
- Provides project cost excursions from:
  – Near-term budget execution impacts
  – External budget changes and constraints
- Documents cost basis and risk impacts.

Pre-Risk Assessment Activities. The RMP may describe the actions that compose this activity. Typically, an IPT may conduct a quick-look assessment of the project to identify the need for technical experts (who are not part of the team) and to examine areas that appear most likely to contain risk. The project's risk coordinator, or an outside expert, may train the IPTs, focusing on the project's risk strategy, definitions, suggested techniques, documentation, and reporting requirements. Section 6.8, Risk Management Training, provides some suggestions for training.

Risk Identification Activity. To identify risk events, IPTs should break down project elements to a level where they, or subject-matter experts, can perform valid assessments. The information necessary to do this varies according to the phase of the project. During the early phases, requirement, threat documents, and acquisition plans may be the only project-specific data available. They should be analyzed to identify events that may have adverse consequences/impacts. A useful initial identification exercise is to perform a mission profile for the system as suggested in DoD 4245.7-M, *Transition from Development to Production*. Using this methodology, the developer creates a functional and environmental profile for the system and examines the low-level requirements that the system must meet to satisfy its mission requirements. The IPTs may then study these requirements to determine which are critical. For example, in an aircraft profile, it may be apparent that high speed is critical. If the speed requirement is close to that achieved by existing aircraft, this may not be a concern. However, if the speed is greater than that achieved by today's aircraft, it may be a critical risk area. Since aircraft speed depends, among other things, on weight and engine thrust, it would be desirable to enlist the help of a materials expert to address weight and an engine expert to assess engine-associated risk.

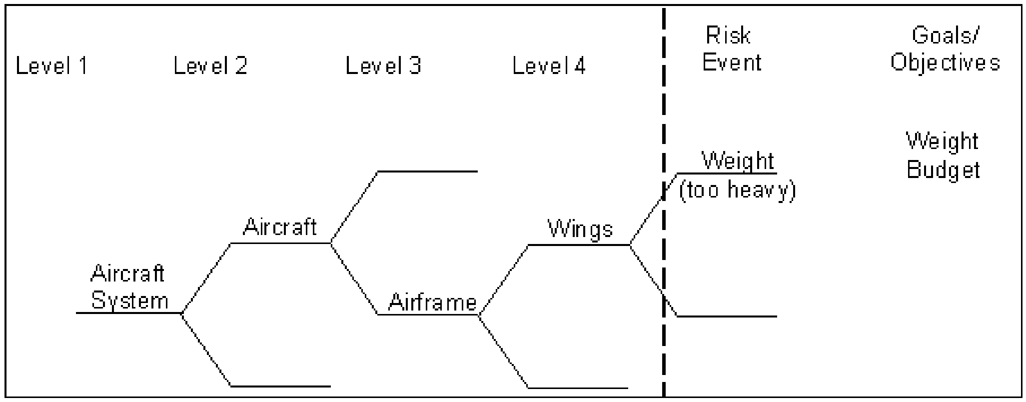


Figure 5. Example of a WBS Dependent Evaluation Structure

Another method of decomposition is to create a WBS as early as possible in a project. Figure 5 is a simple example of a decomposition, based on the WBS for an aircraft. The figure shows an important requirement of the decomposition process, the establishment of goals (e.g., don't exceed the weight budget or objective). Risk events are determined by matching each WBS element and process to sources or areas of risk.

During decomposition, risk events are identified from experience, brainstorming, lessons learned from similar programs, and guidance contained in the RMP. A structured approach previously discussed matches each WBS element and process in terms of sources or areas of risk. The examination of each element against each risk area is an exploratory exercise to identify the critical risks. The investigation may show that risks are interrelated. For example, the weight of an aircraft affects its speed, but also impacts the payload, range, and fuel requirements. These have design and logistics consequences/impacts and may even affect the number of aircraft that must be procured to meet objectives.

Critical risks need to be documented as specified in the RMP and may include the scenario that causes the risk, planned management controls and actions, etc. It may also contain an initial assessment of the consequences/impacts to focus the risk assessment effort. A risk watch list should be initiated as part of risk identification. It is refined during handling, and monitored/updated during the monitoring phase.

Risk Analysis Activity. Analysis begins with a detailed study of the critical risk events that have been identified. The objective is to gather enough information about the risks to judge the probability of occurrence and the impact on cost, schedule, and performance if the risk occurs.

Impact assessments are normally subjective and based on detailed information that may come from:

- Comparisons with similar systems
- Relevant lessons-learned studies
- Experience

- Results from tests and prototype development
- Data from engineering or other models
- Specialist and expert judgments
- Analysis of plans and related documents
- Modeling and simulation
- Sensitivity analysis of alternatives.

Depending on the particular technique and the risk being analyzed, some supporting analysis may be necessary, i.e., analysis of contractor processes, such as design, engineering, fault tree analysis, engineering models, simulation, etc. Analyses provide the basis for subjective assessments.

A critical aspect of risk analysis is data collection. Two primary sources of data are interviews of subject-matter experts and analogy comparisons with similar systems. Section 6.3 contains a procedure for collecting both types of data for use in support of the techniques listed in Table 1. Periodically, sets of risks need to be prioritized in preparation for risk handling, and aggregated to support program management reviews. Section 6.4, Risk Prioritization, describes methods for accomplishing this.

Table 1. Risk Assessment Approaches

Risk Assessment Technique	Applicable Acquisition Phases	Applicable Risk Areas & Processes
Plan Evaluation/Risk Identification	All phases	Project Plans and critical communications with the developer
Product (WBS) Risk Assessment	All phases starting with the completion of the Contract WBS	All critical risk areas except threat, requirements, cost, and schedule
Process (DoD 4265.7-M) Risk Assessment	All phases, but mainly late SDD	All critical risk processes
Cost Risk Assessment	All phases	Cost critical risk areas
Schedule Risk Assessment	All phases	Schedule critical risk areas

Table 2. Probability/Likelihood Criteria (Example)

Level	What is the Likelihood the Risk Event Will Happen?
a	Remote
b	Unlikely
c	Likely
d	Highly likely
e	Near certainty

Table 3. Consequences/Impacts Criteria (Example)

Level	Given the Risk Is Realized, What Is the Magnitude of the Impact?		
	Performance	**Schedule**	**Cost**
a	Minimal or no impact	Minimal or no impact	Minimal or no impact
b	Acceptable with some reduction in margin	Additional resources required; able to meet need dates	<5%
c	Acceptable with significant reduction in margin	Minor slip in key milestones; not able to meet need date	5-7%
d	Acceptable; no remaining margin	Major slip in key milestone or critical path impacted	7-10%
e	Unacceptable	Can't achieve key team or major program milestone	>10%

Table 4. Overall Risk Rating Criteria (Example)

Risk Rating	Description
High Moderate Low	Major disruption likely Some disruption Minimum disruption

Table 5. Risk Ratings (Example)

Priority	Area/Source Process	Location	Risk Event	Probability	Consequence	Risk Rating
1	Design	WBS 3.1	Design not completed on time	Very likely	Severe	High
2						
3						

Risk Rating and Prioritization/Ranking

Risk ratings are an indication of the potential impact of risks on a program; they are a mea-sure of the probability/likelihood of an event occurring and the consequences/impacts of the event. They are often expressed as high, moderate, and low. Risk rating and prioritization/ranking are considered integral parts of risk analysis.

A group of experts, who are familiar with each risk source/area (e.g., design, logistics, production, etc.) and product WBS elements, are best qualified to determine risk ratings. They should identify rating criteria for review by the PD/PM, who includes them in the RMP. In most cases, the criteria will be based on the experience of the experts, as opposed to mathematically derived, and should establish levels of probability/likelihood and consequences/impacts that will provide a range of possibilities large enough to distinguish differences in risk ratings. At the project level, consequences/impacts should be expressed in terms of impact on cost, schedule and performance. Tables 2 and 3 are examples of probability/likelihood and consequence/impact criteria, and Table 4 contains an example of overall risk rating criteria, which considers both probability/likelihood and consequences/impacts. Table 5 provides a sample format for presenting risk ratings.

Using these risk ratings, PDs/PMs can identify events requiring priority management (high or moderate risk probability/likelihood or consequences/impacts). The document prioritizing the risk events is called a Watch List. Risk ratings also help to identify the areas that should be reported within and outside the PD/PM, e.g., milestone decision reviews. Thus, it is important that the ratings be portrayed as accurately as possible.

A simple method of representing the risk rating for risk events, i.e., a risk matrix, is shown in Figure 6. In this matrix, the PD/PM has defined high, moderate, and low levels for the various combinations of probability/likelihood and consequences/impacts.

Likelihood					
e	L	M	H	H	H
d	L	M	M	H	H
c	L	M	M	M	H
b	L	L	L	M	M
a	L	L	L	L	M
	a	b	c	d	e
	Consequence				

Figure 6. Overall Risk Rating (Example)

There is a common tendency to attempt to develop a single number to portray the risk associated with a particular event. This approach may be suitable if both probability/likelihood (probability) and consequences/impacts have been quantified using compatible cardinal scales or calibrated ordinal scales whose scale levels have been determined using accepted procedures (e.g., Analytical Hierarchy Process). In such a case, mathematical manipulation of the values may be meaningful and provide some quantitative basis for the ranking of risks.

In most cases, however, risk scales are actually just raw (uncalibrated) ordinal scales, reflecting only relative standing between scale levels and not actual numerical differences. Any mathematical operations performed on results from uncalibrated ordinal scales, or a combination of uncalibrated ordinal and cardinal scales, can provide information that will at best be misleading, if not completely meaningless, resulting in erroneous risk ratings. Hence, mathematical operations should generally not be performed on scores derived from uncalibrated ordinal scales. (Note: risk scales that are expressed as decimal values (e.g., a 5 level scale with values 0.2, 0.4, 0.6, 0.8 and 1.0) still retain the ordinal scale limitations discussed above.)

One way to avoid this situation is to simply show each risk event's probability/likelihood and consequences/impacts separately, with no attempt to mathematically combine them. Other factors that may significantly contribute to the risk rating, such as time sensitivity or resource availability, can also be shown. The prioritization or ranking—done after the rating—should also be performed using a structured risk rating approach (e.g., Figure 6) coupled with expert opinion and experience. Prioritization or ranking is achieved through integration of risk events from lower to higher WBS levels. This means that the effect of risk at lower WBS elements needs to be reflected cumulatively at the top or system level.

3.6 Risk Handling

3.6.1 Purpose of Risk Handling

Risk handling includes specific methods and techniques to deal with known risks and a schedule for accomplishing tasks, identifies who is responsible for the risk area, and provides an estimate of the cost and schedule associated with handling the risk, if any. It involves planning and execution with the objective of handling risks at acceptable levels. The IPTs that assess risk should begin the process to identify and evaluate handling approaches to propose to the PD/PM, who selects the appropriate ones for implementation.

3.6.2 Risk-Handling Process

The risk-handling phase must be compatible with the RMP and any additional guidance the PD/PM provides. A critical part planning involves refining and selecting of the most appropriate handling options.

The IPTs that evaluate the handling options may use the following criteria as a starting point for assessment:

- Can the option be feasibly implemented and still meet the user's needs?
- What is the expected effectiveness of the handling option in reducing project risk to an acceptable level?
- Is the option affordable in terms of dollars and other resources (e.g., use of critical materials, test facilities, etc.)?
- Is time available to develop and implement the option, and what effect does that have on the overall project schedule?
- What effect does the option have on the system's technical performance?

Risk-handling options can include risk control, risk avoidance, risk assumption, and risk transfer. Although the control risk-handling option is commonly used in DOE projects, it should not automatically be chosen. All four options should be evaluated and the best one chosen for a given risk issue.

Risk control does not attempt to eliminate the source of the risk but seeks to reduce or mitigate the risks. It monitors and manages the risk in a manner that reduces the probability/likelihood and/or consequence/impact of its occurrence or minimizes the risk's effect on the project. This option may add to the cost of a project; however, the selected approach should provide an optional risk among the candidate approaches of risk reduction, cost effectiveness, and schedule impact. A sampling is listed below of the types of risk control actions available to the PD/PM. Section 6.5.2 discusses them in more detail.

- ***Multiple Development Efforts.*** Create competing systems in parallel that meet the same performance requirements.
- ***Alternative Design.*** Create a backup design option that uses a lower risk approach.
- ***Trade Studies.*** Arrive at a balance of engineering requirements in the design of a system.
- ***Early Prototyping.*** Build and test prototypes early in the system development.
- ***Incremental Development.*** Design with the intent of upgrading system parts in the future.
- ***Technology Maturation Efforts.*** Normally, technology maturation is used when the desired technology will replace an existing technology which is available for use in the system.
- ***Robust Design.*** This approach, while it could be more costly, uses advanced design and manufacturing techniques that promote quality through design.
- ***Reviews, Walk throughs, and Inspections.*** These three actions can be used to reduce the probability/likelihood and potential consequences/impacts of risks through timely assessment of actual or planned events.
- ***Design of Experiments.*** This engineering tool identifies critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.
- ***Open Systems.*** Carefully selected commercial specifications and standards whose use can result in lower risks.
- ***Use of Standard Items/Software Reuse.*** Use of existing and proven hardware and software, where applicable, can substantially reduce risks.
- ***Two-Phase Development.*** Incorporation of formal risk reduction into project research and development. The first part of research and development is where prototypes are developed and tested. In the second part, models or pilot plant are developed and tested.
- ***Use of Mock-ups.*** The use of mock-ups, especially man-machine interface mock-ups, can be used to conduct early exploration of design options.
- ***Modeling/Simulation.*** Modeling and simulation can be used to investigate various design options and system requirement levels.

- ***Key Parameter Control Boards.*** *Th*e practice of establishing a control board for a parameter may be appropriate when a particular feature (such as system weight) is crucial to achieving the overall program requirements.
- ***Manufacturing Screening.*** For projects in research and development, various manufacturing screens can be incorporated into test article production and low rate initial production to identify deficient manufacturing processes.

Risk avoidance involves a change in the concept, requirements, specifications, and/or practices that reduce risk to an acceptable level. Simply stated, it eliminates the sources of high or possibly medium risk and replaces them with a lower risk solution and may be supported by a cost/benefit analysis. Generally, this method may be done in parallel with the up-front requirements analysis, supported by cost/requirement trade studies, which can include cost-as-an-independent-variable trades.

Risk Assumption. Risk assumption is an acknowledgment of the existence of a particular risk situation and a conscious decision to accept the associated level of risk, without engaging in any special efforts to control it. However, a general cost and schedule reserve may be set aside to deal with any problems that may occur as a result of various risk assumption decisions. This method recognizes that not all identified project risks warrant special handling; as such, it is most suited for those situations that have been classified as low risk. The key to successful risk assumption is twofold:

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it materializes. This includes identifying the specific management actions (such as retesting, additional time for further design activities) that may occur.
- Ensure that necessary administrative actions are taken to identify a management reserve to accomplish those management actions.

Risk-handling options have broad cost implications. The magnitude of these costs is circumstance-dependent. The approval and funding of handling options should be part of the process that establishes the program cost and performance goals. This should normally be done by the project IPT. The selected handling option should be included in the project's acquisition strategy.

Once the acquisition strategy includes risk-handling approaches, the PD/PM can derive the schedule and identify cost, schedule, and performance, impacts to the basic project.

Risk Transfer. This action may reallocate risk during the concept development and design processes from one part of the system to another, thereby reducing the overall system risk, or redistributing risks between the Government and the prime contractor or within Government agencies; or between members of the contractor team. It is an integral part of the functional analysis process. Risk transfer is a form of risk sharing and not risk abrogation on the part of the Government, and it may influence cost objectives. An example is the transfer of a function from hardware implementation to software implementation or vice versa. The effectiveness of risk transfer depends on the use of successful system design techniques. Modularity and functional partitioning are two design techniques that support risk transfer. In some cases, risk transfer may concentrate risk areas in one area of the design. This allows management to focus attention and resources on that area.

3.7 Risk Monitoring

The monitoring process systematically tracks and evaluates the effectiveness of risk-handling actions against established metrics. Monitoring results may also provide a basis for developing additional handling options and identifying new risks. The key to the monitoring process is to establish a cost, schedule, and performance management indicator system over the entire project that the PD/PM uses to evaluate the status of the project. The indicator system should be designed to provide early warning of potential problems to allow management actions. Risk monitoring is not a problem-solving technique, but rather, a proactive technique to observe the results of risk handling and identify new risks. Some monitoring techniques can be adapted to become part of a risk indicator system:

- ***Test and Evaluation.*** A well-defined test and evaluation program is a key element in monitoring the performance of selected risk-handling options and developing new risk assessments.
- ***Test-Analyze-and-Fix.*** Test-Analyze-and-Fix is the use of a period of dedicated testing to identify and correct deficiencies in a design.
- ***Demonstration Events.*** Demonstration events are points in the project (normally tests) that determine if risks are being successfully abated.
- ***Earned Value.*** This uses standard cost/schedule data to evaluate a project's cost and schedule performance in an integrated fashion. As such, it provides a basis to determine if risk-handling actions are achieving their forecasted results.
- ***Technical Performance Measurement.*** Technical Performance Measurement is a product design assessment which estimates, through engineering analysis and tests, the values of essential performance parameters of the current design as effected by risk-handling actions.
- ***Project Metrics.*** These are used for formal, periodic performance assessments of the various development processes, evaluating how well the system development process is achieving its objective. This technique can be used to monitor corrective actions that emerged from an assessment of the critical risk processes.
- ***Process Proofing.*** Similar to project Metrics, but aimed at manufacturing and support processes which are critical to achieving system requirements. Proofing simulates actual production environments and conditions to insure repeatedly conforming hardware and software.

- ***Schedule Performance Monitoring.*** This is the use of program schedule data to evaluate how well the project is progressing to completion.

Section 6.6 describes several monitoring techniques, e.g., earned value.

The indicator system and periodic reassessments of project risk should provide the PD/PM with the means to incorporate risk management into the overall project management structure.

3.8 Risk Documentation

A primary criterion for successful management is formally documenting the ongoing risk management process. This is important because:

- It provides the basis for program assessments and updates as the project progresses
- Formal documentation tends to ensure more comprehensive risk assessments than undocumented efforts
- It provides a basis for monitoring risk-handling actions and verifying the results
- It provides project background material for new personnel
- It is a management tool for the execution of the project
- It provides the rationale for project decisions.

Documentation should be done by those responsible for planning and collecting and analyzing data, i.e., IPT-level in most cases.

Risk management reports vary depending on the size, nature, and phase of the project. Examples of some risk management documents and reports that may be useful to a PD/PM are:

- Risk Management Plan
- Risk information form
- Risk assessment report
- Risk handling priority list
- Risk handling plan of action
- Aggregated risk list
- Risk monitoring documentation:
    - Project metrics
    - Technical reports
    - Earned value reports
    - Watch list
    - Schedule performance report

— Critical risk processes reports.

Most PDs/PMs can devise a list of standard reports that will satisfy their needs most of the time. However, since there will always be a need for ad hoc reports and briefing and assessments, it is advisable to store risk information in a management information system. This allows deriving standard reports and creating of ad hoc reports, as needed.

Acquisition reform discourages Government oversight; therefore, formal contractor-produced risk documentation may not be available for most projects. However, project insight is encouraged, and PDs can obtain information about project risk from contractor internal documentation such as:

- *Risk Management Policy and Procedures*. This is a description of the contractor's corporate policy for the management of risk. The procedures describe the methods for risk identification, analysis, handling, monitoring, and documentation. It should provide the baseline planning document for the contractor's approach to risk management.
- *Corporate Policy and Procedures Documents.* Corporations have policy and procedures documents that address the functional areas that are critical to the design, engineering, manufacture, test and evaluation, quality, configuration control, manufacture, etc., of a system. These documents are based on what the company perceives as best practices, and although they may not specifically address risk, deviation from these policies represents risk to a project. Internal company reports that address how well projects comply with policy may be required and will provide valuable information.
- *Risk Monitoring Report*. Contractors should have internal tracking metrics and reports for each moderate-or high-risk item. These metrics may be used to determine the status of risk reduction programs.

4.0 RISK MANAGEMENT AND THE ACQUISITION PROCESS

This Section discusses the relationship between risk and the acquisition process, describes how risk is considered in design of the Acquisition Strategy, and expresses the need to consider risk as early in the program as possible.

4.1 Overview

The DOE acquisition process for the management of projects consists of a series of phases designed to reduce risk, ensure affordability, and provide adequate information for decision-making. Acquisition officials are encouraged to tailor projects to eliminate phases or activities that result in little payoff in fielding time or cost savings. To effectively tailor a project, one needs to understand the risks present in the project and to develop a plan for managing these risks. DOE policy calls for the continual assessment of project risks, beginning with the initial phase of an acquisition project, and the development of management approaches before any decision is made to enter all subsequent phases.

The application of risk management processes (planning, assessment, identification, analysis, handling, and monitoring) is particularly important during the research and development phase of any project, when alternatives are evaluated, project objectives are established, and the acquisition strategy is developed. All of these activities require acceptance of some level of risk and development of plans to manage the risk.

As a project evolves into subsequent phases, the nature of the risk management effort will change. New assessments will be built on previous ones. Risk areas will become more specific as the system is defined.

Risk management should also be an integral part of any source selection process, from request for proposals preparation, through proposal evaluation, and after contract award. Throughout the project life, the IPT will play a key role in risk management activities.

4.2 DOE Acquisition Process

The phases and milestones of the acquisition process provide a streamlined structure that emphasizes risk management and affordability. The phases are a logical means of progressively translating broadly stated mission needs into well-defined system-specific requirements, and ultimately into operationally effective, suitable, and survivable systems. The term “system” includes hardware, software, and the human element. Each phase is designed, among other things, to manage risks. Milestones are points in time that allow decision makers to evaluate the program status and determine if the project should proceed to the next phase. The Acquisition Executive (AE) and PD tailor milestones and phases so that each milestone decision point allows assessment of project status and the opportunity to review plans for the next phase and beyond. The AE should explicitly address project risks and the adequacy of risk management planning during the milestone reviews and establish exit criteria for progression to the next phase.

The contract schedule normally allows time for milestone decisions before spending begins in subsequent phases and should also permit demonstration of the exit criteria in time to support the milestone review. There are exceptions to this—driven by funding availability and option award dates. However, the objective is to provide proper fiscal control without delaying the acquisition decisions or contracts while adequately considering risk.

The acquisition strategy defines the business and technical management approach to meet objectives within project constraints with a primary goal to minimize the time and cost of satisfying a valid need, consistent with common sense and sound business practices. The Program Manager or the PD prepares a preliminary acquisition strategy as an Initiation phase activity that focuses on identifying risk and handling options. Later, the PD updates the strategy to support each milestone decision by describing activities and events planned for the upcoming phase and relating the accomplishments of that phase to the project’s overall, long-term objectives. Identified project risks will significantly influence the acquisition strategy.

4.3 Characteristics of the Acquisition Process

The acquisition process that has evolved can be characterized in terms of the following concepts that are particularly relevant to the management of risk in projects.

4.3.1 Integrated Product and Process Development

Integrated product and process development integrates all acquisition activities in order to optimize system development, production, and deployment. Key to the success of the integrated product and process development is the IPT, which is composed of qualified and empowered representatives from all appropriate functional disciplines who work together to identify and resolve issues. As such, the IPT is the foundation for organizing for risk management.

4.3.2 Continuous Risk Management

PDs/PMs should focus on risk management throughout the life of the project, not just in preparation for project and milestone reviews. Project risks should be continuously assessed, and the risk-handling approaches developed, executed, and monitored throughout the acquisition process. Both the Government and contractors must understand risks as a project progresses through the various phases and milestone decision points, and must modify the management strategy and plan accordingly. While specific Government and contractors risk management processes may likely be different, it is important that each party have a common and complete set of process steps (regardless of their names), and be able to exchange and clearly understand the other party’s risk management documentation.

4.3.3 Stability

Once a project is initiated, project stability is a top priority. Keys to creating project stability are realistic investment planning and affordability assessments. They must reflect an accurate and comprehensive understanding of existing or expected project risks. A risk management strategy must be developed early in the process, before actually initiating the project to ensure it is a stable one, recognizing that key issues affecting project stability may be external.

4.3.4 Reduction of Life Cycle Costs

DOE considers the reduction of total cost to acquire and operate systems while maintaining a high level of performance for the user to be of highest priority. Aggressive, and realistic cost objectives are set early in an acquisition project and then all aspects of the project are managed to achieve those objectives, while still meeting the user’s performance and schedule needs. Inherent in this process is the realization that risks must be understood, taken, and managed in order to achieve cost, schedule, and performance objectives. An understanding of risk is essential to setting realistic cost objectives. The PD/PM and user representatives should identify risk and cost driving requirements during the generation of the requirements document in order to know where tradeoffs may be necessary.

4.3.5 Event-Oriented Management

Event-oriented management requires that decision-makers base their decisions on significant events in the acquisition life cycle, rather than on arbitrary calendar dates. This management process emphasizes effective acquisition planning and embodies sound risk management. Decisions to proceed with a project should be based on demonstration of performance, through test and evaluation, and on verification that project risks are well understood and are being managed effectively. Attainment of agreed-upon exit criteria is an indication that the PD/PM is managing risk effectively.

4.3.6 Modeling and Simulation

Properly used, models and simulations can reduce time, resources, and acquisition risk and may increase the quality of the systems being developed. Users of these models and simulations must have a good understanding of their capabilities and limitations and their applicability to the issues being addressed.

From a risk perspective, modeling and simulation may be used to:

- Develop alternative concepts during system design, predict performance in support of trade-off studies
- Evaluate system design and support preliminary design reviews during design development
- Predict system performance and supplement live tests during testing
- Examine the value of the system,
- Determine the impact of design changes, hone requirements
- Develop life cycle support requirements and assessments.

However, a key limitation through models and simulations is that the results are only as accurate and certain as the quality of the underlying relationships and input data. Blindly believing and using the output from models and simulations should never be done.

4.4 Risk Management Activities During Acquisition Phases

Risk management activities should be applied continuously throughout all acquisition process phases. However, because of the difference in available information, the level of application and detail will vary for each phase. In the Initiation phase, management focuses on assessing the risks in the alternative concepts available to satisfy users needs and on planning a strategy to address those risks. For each of the subsequent phases, all four risk management activities may be applied with increasing focus on risk handling and monitoring.

The PD/PM identifies objectives, alternatives, and constraints at the beginning of each phase of a project and then evaluates alternatives, identifies sources of project risk, and selects a strategy for resolving the risks. The PD/PM updates the acquisition strategy, risk assessments, and other aspects of project planning, based on analyses, for the phase of the acquisition.

Developers should become involved in the risk management process at the beginning, when users define performance requirements, and continue during the acquisition process until the system is delivered. The early identification and assessment of critical risks allow PDs/PMs to formulate handling approaches and to streamline the program definition and the request for proposals around critical product and process risks.

The following paragraphs address risk management in the different phases in more detail.

4.4.1 Initiation Phase

The Initiation phase normally consists of studies that define and evaluate the feasibility of alternative concepts and provide the basis for the assessment of these alternatives in terms of their advantages, disadvantages, and risk levels at Critical Decision-0. In addition to providing input to the analysis of alternatives, the PD develops a proposed performance baseline (PB) and exit criteria.

The PB documents the most important performance, cost, and schedule objectives and thresholds for the selected concepts. The parameters selected are such that a re-evaluation of alternative concepts is appropriate if thresholds are not met. Exit criteria are events or accomplishments that allow managers to track progress in critical technical, cost, or schedule risk areas. They must be demonstrated to show that a project is on track.

In defining alternative concepts, PDs/PMs should pay particular attention to the threat and the user's requirements, which are normally stated in broad terms. Risks can be introduced if the requirements are not stable, or if they are overly restrictive and contain specific technical solutions. Requirements can also be significant cost and schedule risk drivers if they require a level of performance that is difficult to achieve within the project budget and time constraints. Such drivers need to be identified as early in the project as possible.

The acquisition strategy should address the known risks for each alternative concept, and the plans to handle them including specific events intended to control the risks. Similarly, the research and development strategy should reflect how research and development will be used to assess risk levels and identify new or suspected risk areas.

A risk management strategy, derived in concert with the acquisition strategy, should be developed during this phase and revised and updated continually throughout the project. This strategy should include risk management planning that clearly defines roles, responsibilities, authority, and documentation for project reviews, risk assessments, and risk monitoring.

4.4.2 Subsequent Phases

During subsequent phases, concepts, technological approaches, and/or design approaches (selected at the previous milestone decisions) are pursued to define the project and project risks. Selected alternative concepts continue to be analyzed, and the acquisition strategy, and the various strategies and plans derived from it, continue to be refined.

Risk management efforts in these phases focus on: understanding critical technology, construction, and support risks, along with cost, schedule, and performance risks; and demonstrating that they are being controlled before moving to the next milestone. Note that the accuracy of cost, schedule, and performance risk assessments should improve with each succeeding project phase (e.g., more info, better design documentation, etc.). Thus, particular attention should be placed on handling and monitoring activities. Planning and assessment should continue as new information becomes available and new risk events are identified.

During these phases, the risk management program should be carried out in an integrated Government-contractor framework to the extent possible, that allows the Government to manage project risks, with the contractor responsible to the PD for product and process risks and for maintaining design accountability. Both the Government and contractors need to understand the risks clearly, and jointly plan management efforts. In any event, risk management needs to be tailored to each project and contract type.

4.5 Risk Management and Milestone Decisions

Before a milestone review, the PD/PM should update risk assessments, explicitly addressing the risks in the critical areas, such as threat, requirements, technology, etc., and identify areas of moderate or high risk.

Each critical technical assessment should be supported by subsystems' risk assessments, which should be supported by design reviews, test results, and specific analyses.

The PD/PM should present moderate- or high-risk mitigation action plans at the milestone review to determine their adequacy and ensure the efficient allocation of resources.

4.6 Risk Management and the Acquisition Strategy

In addition to providing the framework for program planning and execution, the acquisition strategy serves several purposes that are important to risk management:

- Provides a master schedule for research, development, test, production, deployment, and critical events in the acquisition cycle.
- Gives a master checklist of the important issues and alternatives that must be addressed.
- Assists in prioritizing and integrating functional requirements, evaluating alternatives, and providing a coordinated approach to integrate diverse functional issues, leading to the accomplishment of project objectives.

- Documents the assumptions and guidelines that led to project initiation and direction
- Provides the basis for the development and execution of the various subordinate functional strategies and plans.

The strategy structure should ensure a sound project through the management of cost, schedule, and performance risk. A good acquisition strategy acknowledges and identifies project risks and forms the basis for implementing a forward-looking, rather than reactive, effective risk management effort.

The acquisition strategy should describe how risk is to be handled and identify which risks are to be shared with the contractor and which are to be retained by the Government. The key concept here is that the Government shares the risk with the contractor, but does not transfer risk to the contractor. The PD has a responsibility to the system user to develop a capable system and can never be absolved of that responsibility. Therefore, all project risks, whether managed by the PD or by the contractor, must be assessed and managed by the PD.

Once the project office has determined how much risk is to be shared with the contractor, it should assess the total risk assumed by the developing contractor (including subcontractors). The Government should not require contractors to accept financial risks that are inconsistent with their ability to handle them. Financial risks are driven, in large measure, by the underlying technical and programmatic risks inherent in a program. The Government contracting officer should, therefore, select the proper type of contract based on an appropriate risk assessment, to ensure a clear relationship between the selected contract type and project risk. An example would be the use of cost-reimbursable-type contracts for development projects.

4.7 Risk Management and Cost

The intention here is to establish a balance between cost, schedule, performance, and risk early in the acquisition process and to manage to a cost objective—the total project cost (TPC) and PB. PDs are required to establish aggressive cost objectives, defined to some degree by the maximum level of acceptable risk. Risks in achieving both performance and aggressive cost goals must be clearly recognized and actively managed through:

- Continuing iteration of cost/performance/schedule/risk tradeoffs
- Identifying key performance and manufacturing process uncertainties
- Demonstrating solutions before production.

Whereas DOE has traditionally managed performance risk, equal emphasis must be placed on managing cost and schedule risks. An underlying premise is that if costs are too great, and there are ways to reduce them, then the user and developer may reduce performance requirements to meet cost objectives. Cost control and effective risk management involve planning and scheduling events and demonstrations to verify solutions to cost, schedule, performance risk issues.

User participation in the trade-off analysis is essential to attain a favorable balance between cost, schedule, performance, and risk. The PD/PM and user representatives should identify risk and cost driving requirements during the generation requirements to know where tradeoffs may be possible. Risk assessments are critical to the process since they provide users and developers with essential data to assist in the cost, schedule, performance, risk trade decisions.

Cost for risk management is directly related to the level of risk and affects a project in two ways. First, costs are associated with specific handling activities, for example, a parallel development. Second, funds are needed to cover the known risks of the selected system approach (i.e., funds to cover cost uncertainty). PDs/PMs must include the anticipated expense of managing risk in their estimates of project costs. Decision-makers must weigh these costs against the level of risk in reaching project-funding decisions.

5.0 RISK MANAGEMENT AND PROJECT MANAGEMENT

Risk management, as a project management responsibility can be a comprehensive and responsive management tool if it is properly organized and monitored at the PD/PM level. A formalized risk management program should be well planned and forward-looking by identifying, analyzing, and resolving potential problem areas before they occur, and by incorporating monitoring techniques that accurately portray the status of risks and the efforts to mitigate them. Introduction of risk management early in a project emphasizes its importance and encourages contractors and members of the Government team to consider risk in the daily management functions.

This section addresses the relationship between risk management and project management and suggests methods of introducing risk management, organizing for risk, and training.

5.1 Overview

A PD/PM should organize for risk management, using existing IPTs. The PD may also want to use contractors to support management efforts or have experts, not involved with the program, perform independent assessments.

To use risk management as a project management tool, the information resulting from each of the risk processes should be documented in a usable form and available to members of the Government/industry project team. This information will provide the basis for reporting risk and overall program information, both internally and externally. Managing collection and dissemination of risk information can be enhanced through the use of a management information system.

5.2 Project Director and Risk Management

All PDs are responsible for establishing and executing a risk management program that satisfies DOE policies. A PD must balance program-unique requirements or circumstances (e.g., size of the PD staff) against the demands of proven risk management principles and practices. This section addresses these principles and practices and provides a basis for establishing a PD's risk management organization and related procedures. The following guidelines define an approach to risk management.

5.2.1 Risk Management Is a Project Management Tool

Risk management should be integral to a project's overall management. PDs must take an active role in the process to ensure that their approach leads to a balanced use of project resources, reflects their overall management philosophy, and includes Government and contractors. Past practices have generally treated risk management solely as a system engineering function, cost-estimating technique or possibly as an independent function distinct from other project functions. Today, risk management is recognized as a vital integrated project management tool that cuts across the entire acquisition project, addressing and interrelating cost, schedule, and performance risks. The goal is to make everyone involved in a project 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. Specific functional areas—such as system engineering—could be charged with implementing risk management, as long as they take the project management view toward it.

5.2.2 Risk Management Is a Formal Process

Formal risk management refers to a structured process whereby risks are systematically identified, analyzed, handled, and monitored. (A recommended structure is described in Section 2.) A structured risk management process, which is applied early, continuously, and rigorously, provides a disciplined environment for decision-making and for the efficient use of program resources. Through a disciplined process PDs/PMs can uncover obscure and lower-level risks that collectively could pose a major risk.

The need for a formal risk management process arises from the nature of risk and the complexity of acquisition projects. The numerous risks in an acquisition project are often interrelated and obscure and change in the course of the development process. A formal approach is the only effective method to sort through numerous risk events, to identify the risks and their interrelationships, to pinpoint the truly critical ones, and to identify cost-effective ways to reduce those risks, consistent with overall project objectives.

A structured process can reduce the complexity of an acquisition project by defining an approach to assess, handle, monitor, and communicate project risk. The systematic identification, analysis, and mitigation of risks also provides a reliable way to ensure objectivity, that is, minimize unwarranted optimism, prejudice, ignorance, or self-interest. Further, structure reduces the impact of personnel turnover and provides a basis for training and consistency among all the functional areas of a project. A structured risk program may also promote teamwork and understanding and improves the quality of the risk products.

5.2.3 Risk Management Is Forward-Looking

Effective risk management is based on the premise that PDs/PMs must identify potential problems, referred to as risk events, long before they occur and develop strategies that increase the probability/likelihood of a favorable outcome to these problems. This occurs by using analytical techniques that provide forward-looking assessments.

Typically, the early identification of potential problems is concerned with two types of events. The first is relevant to the current or imminent acquisition phase of a project (intermediate-term), such as satisfying a technical requirement in time for the next milestone review. The second is concerned with the future phase(s) of a project (long-term) such as potential risk events related to transitioning a system from development to operation.

By analyzing critical events, certain risks can be determined. To do this, one should consider the range of potential outcomes and the factors that determine those outcomes. Through risk handling, a PD/PM can then develop approaches to minimize risk factors.

The right risk-handling options require a balance between actual available resources and those required to fully implement the options and payoffs (intermediate and long-term).

5.2.4 Risk Management Is Integral to Integrated Product and Process Development

One of the tenets of integrated development is multidisciplinary teamwork through the IPT, which is an integral part of the acquisition oversight and review process. The IPT is a valuable resource to assist in developing a RMP and should be used accordingly. The PD/PM should ensure that the requirements of the IPT are reflected in the plan.

Working with the IPT, the PD/PM can establish the type and frequency of risk management information that an IPT requires, and refine management organization and procedures. This should be done during the initial IPT meetings. IPTs will most likely require information concerning:

- Known risks and their characteristics, e.g., probability of occurrence and consequences/impacts
- Planned risk-handling actions—funded and unfunded
- Achievements in controlling risks at acceptable levels.

The IPT may also require details on the PDs/PM's risk management program, access to the RMP, and the results of specific risk assessments. In addition, PDs/PMs may want to present selected information to the IPT to help substantiate a position or recommendation, e.g., help support a budget request.

5.3 Risk Management Organization

The PM, after determining a preferred management approach, must organize the project office and establish outside relationships in order to manage risk. No particular organizational structure is superior. However, experience provides some insights into the development of effective risk management organizations. PDs/PMs should consider the following discussion in the context of their unique requirements and circumstances and apply those that are suitable to their specific needs.

5.3.1 Risk Management Organizational Structure

A major choice for each PD/PM is whether to have a centralized or decentralized risk management organization. The PD/PM may choose a centralized organizational structure until team members become familiar with both the project and the risk management process. In a centralized approach, the PD/PM establishes a team that is responsible for all aspects of risk management. The team would write a plan, conduct assessments, evaluate risk-handling options, and monitor progress. Although this approach may be necessary early in a project, it tends to minimize the concept that risk management is a responsibility shared by all members of the acquisition team, whether Government or contractor.

The PD/PM may also choose to decentralize. The degree of decentralization depends on the assignment of responsibilities. Some level of centralization is almost always essential for prioritizing risk across the project. A project-level integrating IPT (see Figure 7) or a Risk Management Board may be appropriate for this integrating function.

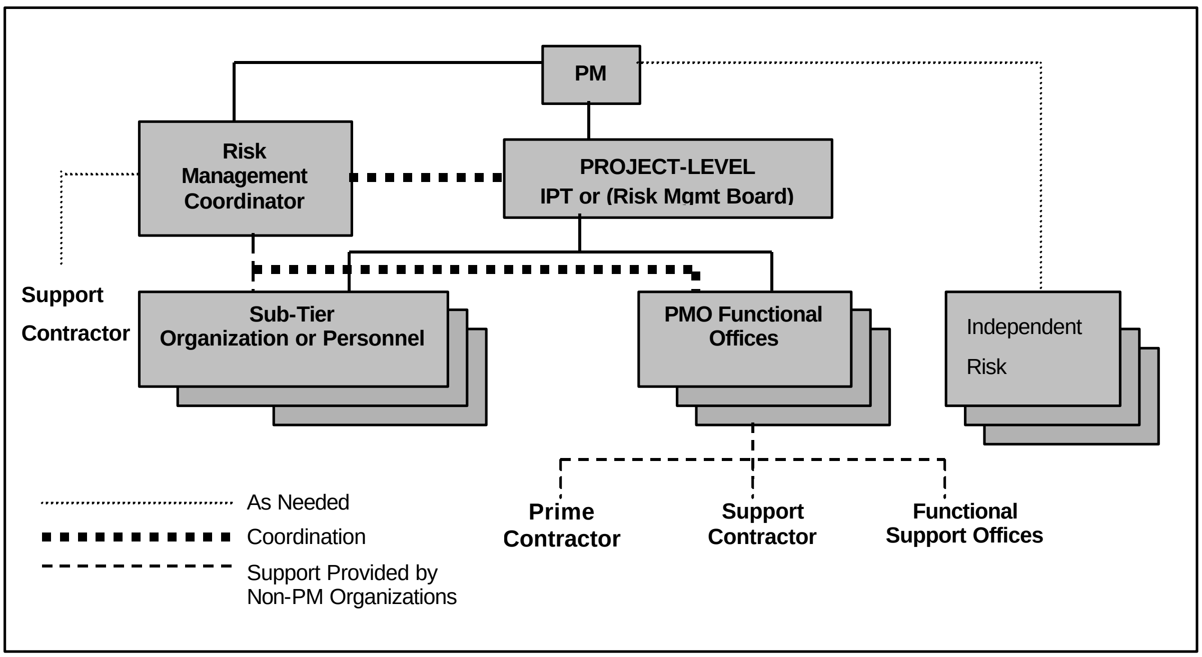


Figure 7. Decentralized Risk Management Organization

The decentralized risk management organization is the recommended approach, and generally results in an efficient use of personnel resources. In this approach, risk management is delegated to IPTs.

The following guidelines apply to all risk management organizations:

- The PD/PM is ultimately responsible for planning, allocating resources, and executing risk management. This requires the PD/PM to oversee and participate in the risk management process.
- The PD/PM must make optimal use of available resources, i.e., personnel, organizations, and funds. Personnel and organizational resources include the PD/PM, functional support offices of the host command, the prime contractor, independent risk assessors, and support contractors.
- Risk management is a team function. This stems from the pervasive nature of risk and the impact that risk-handling plans may have on other project plans and actions. In the aggregate, risk planning, assessment, handling, and monitoring affect all project activities and organizations. Any attempt to implement an aggressive forward-looking risk management program without the involvement of all PD/PM subordinate organizations could result in confusion, misdirection, and wasted resources. The only way to avoid this is through teamwork among the project organizations and the prime contractor. The management organizational structure can promote teamwork by requiring strong connectivity between that structure, the various project organizations, and the prime contractor. The teams may use independent assessments to assist them, when required.

Figure 7 portrays a decentralized risk management organization. This example includes the entire project and selected non-project organizations, e.g., the contractor, may be members of the IPT. The figure shows that risk management is an integral part of project management and not an additional or separate function. Hence, separate personnel are not designated to manage risk, but rather all individuals are required to consider risk management as a routine part of their jobs. In the figure, the risk coordinator reports to the PD/PM, but works in coordination with the project IPT, functional offices, and the project IPT. As shown, this organizational structure is best suited to major system projects, but PDs/PMs can tailor it to satisfy their specific requirements. The details are dependent upon the contract, type, statement of work, and other variable.

The organizational structure shows that the PD/PM is ultimately responsible for risk management. There is a coordinator to assist with this responsibility and act as an “operations” officer. This may be a full-time position or an additional duty, as the PD/PM deems appropriate. The coordinator should have specific training and experience in risk management to increase the chance of successful implementation and to avoid common problems. A support contractor may assist the coordinator by performing administrative tasks associated with that office.

The IPT, composed of individuals from the PD and prime contractor, ensures that the PD’s risk management program is implemented and program results are synthesized into a form suitable for decision-making by the PD/PM and the IPT. The inclusion of both the IPT and project functional offices simply reflects that not all project management functions will be assigned to the IPT for execution.

Independent risk assessors are typically hired when the PD has specific cost, schedule, performance concerns with a hardware or software product or engineering process and wants an independent assessment from an expert in a particular field. The duration of their services is normally short, and tailored to each project.

5.3.2 Risk Management Responsibilities

This Section identifies the primary responsibilities that could be associated with a decentralized risk management organization. In assigning responsibilities to the various organizational elements, the PD/PM should strike a balance between a concentration of responsibilities at higher levels and pushing them too far down the organizational structure.

The development of these responsibilities, in part, is based on the premise that risk management activities must be specific—and assigned to individuals, not groups. The responsibilities listed below are assigned to the leader of each organizational element, recognizing that the composition of each element will be program unique, i.e., number of assigned project personnel, contractor personnel, etc. The task of further assigning these responsibilities, along with tailoring them to satisfy the needs and requirements of each project, remains for PDs/PMs and their staffs to accomplish.

Table 6 provides a description of the responsibilities associated with the decentralized risk management structure, sorted by organizational elements that may make up the risk management structure.

Table 6. Notional Description of Risk Management Responsibilities

Personnel	Job Responsibility
Program Manager	• Plan, organize, direct, and control risk management. • Comply with DOE risk management guidance. • Ensure that funds are available to support approved risk-handling plans. • Inform and advise the IPT on project risk and its mitigation.
Risk Management Coordinator	• Develop and maintain risk management plans. • Provide risk management training. • Define the risk reporting scales to be used by the project. • Develop and maintain a Risk Management Information System. • Prepare risk management reports. • Monitor compliance with DOE risk management requirements. • Ensure risk management functions and tasks performed by the IPT and PD/ PM functional offices are fully integrated and in compliance with assigned tasks • Advise the PD/PM and IPT on the use of risk management sources, i.e., functional support offices, etc. • Evaluate risk assessments, risk-handling plans, and risk monitoring results as directed and recommend appropriate actions. • Advise the PD on the use of independent risk assessors.
Project Level IPT (some PDs/PMs use a Risk Management Board for this Responsibility)	• Ensure that the risk management program is implemented, risk reduction is accomplished in conformance with the PD's/PM's strategy, and the risk management efforts of the IPT are integrated. • Report risk events to the risk management coordinator. • Evaluate whether the IPT and project functional offices have identified critical risks and proposed risk-handling plans. • Ensure that cost, schedule, and performance risks are compatible. • Ensure that cost, schedule, and performance risks are combined in a manner consistent with the plan.
IPT & Functional Offices (Process) and System Elements (Products)	• Assess risks, recommend appropriate risk-handling strategies for identified moderate and high risks, develop, implement, and document all risk management analyses and findings within the team's product area. • Coordinate all risk management findings and decisions with other IPT, project functional offices, and the risk-management coordination office. • Identify funding requirements to implement risk-handling plans. • Identify the need for risk management training. • Report risk events to the AE and risk coordinator.
Independent Risk Assessors	• Perform independent risk assessment on critical risk areas or contractor engineering processes that the PD has specified. • Report the results of those assessments to the PD. • Work with the risk management coordinator.

5.4 Contractor Risk Management

Experience has shown that managing a project's risks requires a close partnership between the PD and the contractor(s). PMs must determine the type of support they need from their contractor, communicate these needs through the request for proposal for each acquisition phase, and then provide for them in the contract. Preparation of the request for proposals and source selection are discussed in subsequent sections.

5.4.1 Contractor View of Risk

Contractors treat risk differently from the Government because each views risk from a different perspective. The PD, in executing his risk management program, needs to understand the contractor viewpoint.

Contractors typically divide risks into two basic types: business risks and project risks. Business risk, in the broadest sense, involves the inherent chance of making a profit or incurring a loss on any given contract. Project risk involves, among other things, technical, requirement, and design uncertainties. A contractor's efforts to minimize business risks may conflict with a PD's efforts to lower project risk.

While the Government and contractors may have different views on specific cost, schedule, and performance risk levels/ratings, they generally have (or should have) similar views of the risk management process. One exception may be the requirements placed by corporate management—that could conflict with the Government view of project risk. The similarity, however, does not necessarily lead to the contractor having a competent internal risk management program. As the Project Management Institute handbook points out, "On most (contractor) projects, responsibility for Project Risk is so pervasive that it is rarely given sufficient central attention." As a minimum, it is important that the PD writes the request for proposals asking the contractor to describe its risk management process, including its approach to managing any specific areas.

5.4.2 Government/Contractor Relationship

The contractor's support and assistance is required even though the ultimate responsibility for risk management rests with the PD. Often, the contractor is better equipped to understand the project technical risks than the PD. Both the Government and contractor need to share information, understand the risks, and develop and execute management efforts. The Government must involve the contractor early in project development, so that effective risk assessment and reduction can occur.

Therefore, risk management must be a key part of the contractor's management scheme. Although the Government does not dictate how the contractor should manage risk, some characteristics of a good Government/contractor relationship include:

- Clear definition of risks and their assignment
- Flexibility for assignment of risks and risk management responsibilities among the teams
- Strong emphasis on best management and technical practices which, if followed, avoid unnecessary risks.

Regarding request for proposals development, discussed later in this section, information is provided on how these characteristics should be addressed.

The Government/contractor partnership can be forged in at least two ways. First, the PD should include the prime contractor(s) in the top-level risk planning and assessment activities. This includes understanding and factoring in such issues as user requirements, affordability constraints, and schedule limitations. Second, the PD should include in advance specific risk assessment and handling tasks as key contractual efforts during the concept exploration and project definition and risk reduction phases.

Forming a joint Government/contractor evaluation team is a good way of fostering an effective partnership. This is especially true in a project's early stages when uncertainty is high and both parties must frequently assess risks. These assessments, properly handled, involve multidisciplinary efforts requiring subject-matter experts from both the contractor and Government. This joint team should evaluate the proposed project in detail and explore the inherent project risks, proposed handling strategies, detailed development schedule, and the contractor's developmental resources (people, facilities, processes, tools, etc.).

A management approach using multiple teams is the best approach to use, e.g., other IPTs. Joint team(s) should be established at the beginning of each development phase to assess the risks to be overcome in that phase and to determine the handling technique(s) to be used. Requirements for contractor participation on the team(s) should be identified in the request for proposals and subsequent contract.

5.5 Risk Management and the Contractual Process

5.5.1 Risk Management: Pre-Contract Award

The contractor's developmental and manufacturing processes and tools, the availability and skill of personnel, and the previous experience of the Government and contractor team all influence their ability to handle the proposed system development and production. Therefore, an effective risk management process includes an evaluation of the capabilities of the potential contractors.

5.5.2 Early Industry Involvement: Industrial Capabilities Review

An industrial capabilities review is a powerful tool available to PDs for determining general industrial capabilities. To avoid potential problems in the subsequent competitive process and to ensure that a "level playing field" is maintained, an announcement in the Commerce Business Daily should be made to inform all potential offerors that the Government plans to conduct a review and to request responses from all interested parties. Below is a general approach that PDs may find readily adaptable to any type of capability review. The basic steps in the process are to:

- Obtain the CO's approval to conduct the review
- Establish the criteria for the capability
- Identify the potential contractors who will participate in the review

- Provide an advance copy of the review material to those contractors
- Select the review team, ensuring that it has the necessary mix of talent
- Train the team on the purpose of the review and review criteria
- Conduct the review and evaluate the results
- Provide feedback to each contractor on the results of their review and assessment
- Provide the results to the PD.

This review is an appraisal of general industrial capabilities and supports identifying potential project risks and best practices rather than evaluating specific contractors.

Regardless of the approach, the PD should determine what specific information is needed. Department of Defense 4245.7-M is a good guide to help tailor a set of questions for the contractors. The questions generally focus on two areas consistent with protection of contractor proprietary information.

- What is the state-of-the-art of the technology proposed for use in the system?
- What are the general developmental/manufacturing capabilities of the potential contractors (including experience, tools, processes, etc.) as compared to industry best practices?

Table 7 shows some of the specific areas or sources for risk identification. It includes a number of areas (threat, requirements, design, etc.) that have been shown through experience to contain risk events that tend to be more critical than others, and which ones should receive the most management attention. Risk events are determined by examining WBS element product and processes in terms of risk areas. Process areas are specifically addressed in Department of Defense 4245.7M. They are general in that areas of risk could be present in any program from either source (WBS or process). They are intended as a list of “top-level” risk sources that will focus attention on a specific area. The PD and contractor(s) will have to examine lower levels to understand the actual risks that are present in their project and to develop an effective management plan. The risks shown are not intended to serve as a simple checklist that one should apply directly, then consider the project risk-free if none of the listed risks are present.

Table 7. Significant Risks by Critical Risk Areas

Risk Area	Significant Risks
Threat	• Uncertainty in threat accuracy. • Sensitivity of design and technology to threat. • Vulnerability of system to threat and threat countermeasures. • Vulnerability of project to intelligence penetration.
Requirements	• Operational requirements not properly established or vaguely stated. • Requirements are not stable. • Required operating environment not described. • Requirements do not address logistics and suitability. • Requirements are too restrictive—identify specific solutions that force high cost.

Risk Area	Significant Risks
Design	• Design implications not sufficiently considered in concept exploration. • System will not satisfy user requirements. • Mismatch of user manpower or skill profiles with system design solution or human-machine interface problems. • Increased skills or more training requirements identified late in the acquisition. • Design not cost effective. • Design relies on immature technologies or “exotic” materials to achieve performance objectives. • Software design, coding, and testing.
Test and Evaluation	• Test planning not initiated early in program (Initiation Phase). • Testing does not address the ultimate operating environment. • Test procedures don’t address all major performance and suitability specifications • Facilities not available to accomplish specific tests, especially system-level tests. • Insufficient time to test thoroughly.
Simulation	• Same risks as contained in the Significant Risks for Test and Evaluation. • M&S are not verified, validated, or accredited for the intended purpose. • Project lacks proper tools and modeling and simulation capability to assess alternatives.
Technology	• Project depends on unproved technology for success—there are no alternatives. • Project success depends on achieving advances in state-of-the-art technology. • Potential advances in technology will result in less than optimal cost-effective system or make system components obsolete. • Technology has not been demonstrated in required operating environment. • Technology relies on complex hardware, software, or integration design.
Logistics	• Inadequate supportability late in development or after fielding, resulting in need for engineering changes, increased costs, and/or schedule delays. • Life cycle costs not accurate because of poor logistics support analyses. • Logistics analyses results not included in cost-performance tradeoffs. • Design trade studies do not include supportability considerations.
Construction/ Production/ Facilities	• Construction/production implications not considered during concept exploration. • Construction/production not sufficiently considered during design. • Inadequate planning for long lead items and vendor support. • Construction/production processes not proven. • Contractors do not have adequate plans for managing subcontractors. • Sufficient facilities not readily available for cost-effective production. • Contract offers no incentive to modernize facilities or reduce cost.
Concurrency	• Immature or unproven technologies will not be adequately developed before construction/production. • Production funding will be available too early—before development effort has sufficiently matured. • Concurrency established without clear understanding of risks.
Capability of Developer	• Developer has limited experience in specific type of development. • Contractor has poor track record relative to costs and schedule. • Contractor experiences loss of key personnel. • Contractor relies excessively on subcontractors for major development efforts. • Contractor will require significant capitalization to meet project requirements.
Cost/Funding	• Realistic cost objectives not established early. • Marginal performance capabilities incorporated at excessive costs-satisfactory, cost performance tradeoffs not done. • Excessive life cycle costs due to inadequate treatment of support requirements.

Risk Area	Significant Risks
	• Significant reliance on software. • Funding profile does not match acquisition strategy.
Schedule	• Funding profile not stable from budget cycle to budget cycle. • Schedule not considered in trade-off studies. • Schedule does not reflect realistic acquisition planning. • PB schedule objectives not realistic and attainable. • Resources not available to meet schedule.
Management	• Acquisition strategy does not give adequate consideration to various essential elements, e.g., mission need, test and evaluation, technology, etc. • Subordinate strategies and plans are not developed in a timely manner or based on the acquisition strategy. • Proper mix (experience, skills, stability) of people not assigned to the project or to contractor team. • Effective risk assessments not performed or results not understood and acted upon.

An examination of the project in these areas can help to develop the final project acquisition strategy and the risk-sharing structure between the Government and industry. The PD can also use the results to adjust the request for proposals for the next phase of the project.

5.5.3 Developing the Request for Proposal

The Request for Proposals should communicate to all offerors the concept that risk management is an essential part of the Government's acquisition strategy.

Before the draft request for proposals is developed using the results of the industrial capabilities review, the PD should conduct a risk assessment to ensure that the project described in the request for proposals is executable within the technical, schedule, and budget constraints. Based on this assessment, a project plan, an integrated master schedule, and life cycle cost estimate may be prepared. The technical, schedule, and cost issues should be discussed in the pre-proposal conference(s) before the draft request for proposals is released. In this way, critical risks inherent in the program can be identified and addressed in the request for proposals. In addition, this helps to establish key risk-management contractual conditions. The request for proposals should encourage offerors to extend the contract WBS to reflect how they will identify all elements at any level that are expected to be high cost or high risk. The request for proposals should also encourage offerors to cite any elements of the contract WBS provided in the draft request for proposals that are not consistent with their planned approach.

In the solicitation, PDs may ask offerors to include a risk analysis and a description of their management plans, and also to develop a supporting project plan and an integrated master schedule in their proposals. These proposals will support the Government's source selection evaluation and the formulation of a most probable cost estimate for each proposal. In addition, the request for proposals may identify the requirement for periodic risk assessment reports that would serve as inputs to the PD's assessment and monitoring processes thereby ensuring that risks are continuously assessed.

5.5.4 *The Offerors Proposal*

The offerors should develop the proposed project plans and documentation at a level that is adequate to identify risks, develop associated management activities that they will use throughout the project, and integrate resources, technical performance measures, and schedule in the proposed project plans. Project plans should extend the contract WBS to reflect the offeror's approach and include the supporting activities, critical tasks, and processes in the contract WBS dictionary. The associated schedules for each should be incorporated into an integrated master schedule. Plans should also have an estimate of the funds required to execute the project and include a breakout of resource requirements for high-risk areas.

The information required and the level of detail will depend on the acquisition phase, the category, and criticality of the project, as well as on the contract type and value. However, the detail submitted with the proposal must be at a sufficiently low level to allow identification of possible conflicts in the planned acquisition approach and to support the Government's proposal evaluation. Generally, the contract WBS should be defined below level 3, by the contractor, only to the extent necessary to capture those lower level elements that are high cost, high risk, or of high management interest.

5.5.5 *Basis for Selection*

DOE acquisition management must focus on balancing cost, schedule, performance, and risk by selecting the contractor team that provides the best value to the user within acceptable risk limits. Therefore, the Request for Proposals/Source Selection process must evaluate each offeror's capability for meeting product and process technical, cost and schedule requirements while addressing and controlling the risks inherent in a project.

The evaluation team should discriminate among offerors based upon the following:

- Risks determined by comparison with the best practices baseline
- Ability to perform with a focus on the critical risk elements inherent in the project
- Adherence to requirements associated with any mandatory legal items
- Past performance on efforts similar to the proposed project being evaluated.

The process of choosing among offerors may be enhanced if the evaluation team includes risk management as a "source selection discriminator." Risk management then becomes an important factor in the Source Selection Authority determination of who provides the most executable program.

5.5.6 *Source Selection*

The purpose of a source selection is to select the contractor whose cost, schedule and performance can best be expected to meet the Government's requirements at an affordable price. To perform this evaluation, the Government must assess both *proposal risk* and *performance risk* for each proposal. These risk assessments must be done entirely within the boundaries of the source selection process. Previous assessments of any of the offerors may not be applicable or allowable.

Proposal Risk. This refers to the risk associated with the *offeror's proposed approach* to meet the Government cost, schedule, and performance requirements. The evaluation of proposal risk includes an assessment of proposed time and resources and recommended adjustments. This assessment should be performed according to the definitions and evaluation standards developed for the source selection. Proposal risk is, in essence, a moderate expansion of past evaluation processes. Historically, evaluators selected contractors who demonstrated that they understood the requirements and offered the best value approach to meeting the Government's needs. The expansion on this concept is the specific consideration of risk.

Technical and schedule assessments are primary inputs to the most probable cost estimate for each proposal. It is important to estimate the additional resources needed to control any risks that have moderate or high risk ratings. Offerors may define them in terms of additional time, personnel requirements, hardware, or special actions such as additional tests. However, whatever the type of the required resources, it is essential that cost estimates be integrated and consistent with the technical and schedule evaluations.

Performance Risk. A performance risk assessment is an evaluation of the contractor's past and present performance record to establish a level of confidence in the contractor's ability to perform the proposed effort. Such an evaluation is not limited to technical issues, but also includes assessment of critical vendor financial viability. Financial capability analyses and industrial capability assessments, conducted in accordance with Department of Defense Handbook 5000.60H, provide insight to a contractor's ability to perform the proposed effort.

A range of methods is available to the PD to evaluate performance risk. Performance risk may be separately assessed for each evaluation factor or as a whole with the assessment provided directly to the source selection advisory authority for final decision or indirectly through the Source Selection Evaluation Board. The assessment relies heavily (although not exclusively) on the contractor performance evaluations and surveys submitted by the PD.

5.6 Risk Management: Post-Contract Award

Post-contract award risk management builds on the work done during the pre-contract award phase. With the award of the contract, the relationship between the Government and the contractor changes as teams are formed to address project risk. These teams should validate pre-contract award management plans by reviewing assessments, handling plans, and monitoring intentions. The extent of assessments increases as the contractor develops and refines his design, test and evaluation, and manufacturing plans. The PD should work with the contractor to refine handling plans.

The process begins with an integrated baseline review after contract award to ensure that reliable plans and performance measurement baselines capture the entire scope of work, are consistent with contract schedule requirements, and have adequate resources assigned to complete project tasks. The reviews could be conducted to incorporate other steps identified below. These steps suggest an approach that the PD might take to initiate the project's risk management plans and activities after contract award. They are intended to be a starting point, and the PD should tailor the plan to reflect each project's unique needs.

- Conduct initial meeting with the contractor to describe the project's objectives and approach to managing risks. The PD may also present the risk management plan.
- Train members of PD and contractor's organization on risk management basics, incorporating the program's management plan and procedures into the training.
- Review the pre-contract award risk plan with the PD and contractor, revise it as necessary, and share results with the contractor.
- Conduct in-depth review of the pre-contract award risk assessments and expand the review to include any new information obtained since the award of the contract.
- Review and revise risk-handling plans to reflect the reassessment of risks.
- Review the project's documentation requirements with the contractor. Ensure that the PD and contractor understand the purpose, format, and contents of various risk reports.
- Initially, it may be necessary to establish a formalized PD-contractor risk management organization for the project, consistent with the terms of the contract.
- Work with the contractor, refine the risk-monitoring plans and procedures.
- Establish the project reporting requirements with the contractor. Describe the Risk Management Information System that the project has established, including procedures for providing information for data entry, and identify reports for the PD and contractor.
- In conjunction with the contractor, identify other risk-management activities that need to be performed.
- Manage the project risk in accordance with the RMP and contract.
- Working with the contractor, refine the risk-monitoring plans and procedures and develop appropriate measures and metrics to track moderate-and high-risk items.

5.7 Risk Management Reporting and Information System

The PD/PM should have a practical method for risk-management reporting, and an information system that supports a risk management program. The reporting needs of the PD/PM establish the type, format, and frequency of information sharing. The IPT concept suggests that the entire team needs access to the risk management information, and the contractor(s) should have access to information, consistent with acquisition regulations. The reporting and information system chosen may be Government-or contractor-owned.

5.8 Risk Management Training

A successful management program depends, to a large extent, on the level of risk management training the PD/PM members and the functional area experts receive. The training will prepare them for critical tasks, such as risk assessments. PDs/PMs will need to organize and conduct principal training for the project office. A three-part framework for training covers project-specific risk management issues, general structure and process, and techniques:

(1) The project-specific training should ensure that everyone has a common vision. It should cover the acquisition strategy, the companion RMP, the PDs/PM's risk-management structure and associated responsibilities, and the management information system.

(2) The following topics provide a starting point for general training syllabus development. The final syllabus should be tailored to meet the program's specific needs. Table 8 provides a list of references that will be useful in developing the syllabus and lesson plans.

- — Concept of Risk
- — Risk Planning
- — Risk Identification
- — Risk Analysis (as applicable)
- — Risk Handling
- — Risk Monitoring.

(3) The third area of training concerns risk-management techniques, concentrating on the techniques the PD/PM plans to employ. The training should focus on how to use the techniques and should include examples of their use. Section 6, Risk Management Techniques, provides a starting point. It contains a general discussion of a set of techniques that address all elements of the risk management process. The discussion of each technique contains a list of references that provide a more in-depth description of the technique. The set of techniques is not exhaustive and the project office should add to the list, if necessary.

Table 8. Risk Management Reference Documents

Document	Description
Department of Defense 4245.7-M, *Transition from Development to Production,* September 1985.	Provides a structure for identifying technical risk areas in the transition from a program's development to production phases. The structure is geared toward development programs but, with modifications, could be used for any acquisition program. The structure identifies a series of templates for each of the development contractor's critical engineering processes. The template includes potential areas of risk and methods for reducing risk in each area.
Risk Management Concepts and Guidance, Defense Systems Management College, March 1989. (Superseded by this *Risk Management Guide*.)	Devoted to various aspects of risk management.
Systems Engineering Management Guide, Defense Acquisition University Press, January 2001, Section 15.	Devoted to risk analysis and management and provides a good overview of the risk management process.
Continuous Risk Management Guide, Software Engineering Institute, Carnegie Mellon University, 1996.	Provides a risk management methodology similar to the one described in the *Deskbook*. Its value is that is subdivides each process into a series of steps; this provides useful insights. Appendix A describes 40 risk-management techniques, the majority of which are standard management techniques adapted to risk management. This makes them a useful supplement to the *Deskbook* identified techniques.
A Systems Engineering Capability Maturity Model, Version 1.0 Software Engineering Institute (Carnegie Mellon University), Handbook SECMM-94-04, December 1994.	Describes one approach to conducting an Industry Capabilities Review. Section PA 10 (pp. 4-72–4-76) discusses software risk management. The material presented in this handbook also can be tailored to apply to system and hardware risk.
A Software Engineering Capability Maturity Model, Version 1.01 Software Engineering Institute (Carnegie Mellon University), Technical Report, December 1996.	Describes an approach to assess the software acquisition processes of the acquiring organization and identifies areas for improvement.
Capability Maturity Model for Software (SM-CMM), Version 1.1,/CMU/SEI-93-TR-24, February 1993.	This is a tool that allows an acquiring organization to assess the software capability maturity of an organization.
Taxonomy-Based Risk Identification, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-93-TR-6 (ESC-TR-93-183, June 1993.	Describes a method for facilitating the systematic and repeatable identification of risks associated with the development of a software-intensive project. This method has been tested in active Government-funded defense and civilian software development projects. The report includes macro-level lessons learned from the field tests.
NAVSO P-6071.	Navy "best practices" document with recommended implementations and further discussion on the material in DoD 4245.7-M.
Risk Management, AFMC Pamphlet 63-101, July 1997.	An excellent pamphlet on risk management that is intended to provide PDs/PMs and IPT with a basic understanding of the terms, definitions, and processes associated with effective risk management. It is very strong on how to perform pre-contract award risk management.

Document	Description
Defense Acquisition Deskbook	Primary reference tool for defense acquisition work force; contains over 1,000 mandatory and discretionary publications and documents which promulgate acquisition policy and guidance. (http://www.deskbook.osd.mil)
Acquisition Software Development Capability Evaluation, AFMC Pamphlet 63-103, 15 June 94.	Describes one approach to conducting an Industry Capabilities Review. This two-volume pamphlet was generated from material originated at Aeronautical Systems Center. The concepts support evaluations during source selection and when requested by IPTs. The material presented in this pamphlet also can be tailored to apply to system and hardware risk management.
Risk Management Critical Process Assessment Tool, Air Force SMC/AXD, Version 2, 9 June 1998.	Provides guidance and extensive examples for developing Request for Proposals Sections "L" and "M," plus source selection standards or risk management. Also includes technical evaluation and review questions, which are helpful for assessing a risk management process; and risk trigger questions, which are helpful for risk identification.
NAVSO P-3686, *Top Eleven Ways to* Manage Technical Risk, October 1998.	Contains the Navy approach to risk management with baseline information, explanations, and best practices that contribute to a well-founded technical risk management program.

6.0 RISK MANAGEMENT TECHNIQUES

This Section provides top-level information on a number of techniques currently used and a combination of techniques used by the industry, and academia. Collectively, they focus on the components of the risk management process and address critical risk areas and processes. The write-ups describe the techniques and give information on their application and utility. The descriptions are at a level of detail that should permit potential users to evaluate the suitability of the techniques for addressing their needs; however, the material does not, in most cases, provide all the information that is required to use a technique. Readers will find that if a particular technique looks promising, they can obtain enough information from the references and tools that will enable project offices to apply them. The descriptions are in a format that aids comparison with other approaches.

6.1 Overview

Techniques are available to support risk management activities. None are required but some have been successfully used in the past. Many of the techniques support processes that are part of sound management and systems engineering and give PDs/PMs the tools for considering risk when making decisions on managing the project.

Several tools have been developed to support each of the components of the risk management process, i.e., planning, assessing, handling, and monitoring and documenting. Although tool developers may claim otherwise, none are integrated to totally satisfy all needs of a PD/PM. Most likely, a PD/PM will choose an overall risk strategy, write a plan to reflect his strategy, review the list of proven techniques to support the components of risk management, assess the techniques against the project's needs and available resources, tailor the techniques to suit the needs of the project, and train program office members to implement the plan.

6.2 Risk Planning Techniques

6.2.1 Description

This technique suggests an approach to risk planning; the process of developing and documenting an organized, comprehensive approach. It also suggests interactive strategy and methods for identifying and tracking risk drivers, developing risk-handling plans, performing continuous assessments to determine how risks have changed, and planning adequate resources. The risk planning technique is applicable to all functional areas in the project, especially critical areas and processes. Using the acquisition strategy as a starting point results in the development of a project risk management strategy, from which flows a management plan that provides the detailed information and direction necessary to conduct an effective management program. This RMP provides the PD/PM with an effective method to define a project, one that fixes responsibility for the implementation of its various aspects, and supports the acquisition strategy.

The technique should first be used in the Initiation phase following the development of the initial acquisition strategy. Subsequently, it may be used to update the PEP on the following occasions: (1) whenever the acquisition strategy changes or there is a major change in project emphasis, (2) in preparation for critical decision points, (3) in preparation for and immediately following technical audits and reviews, (4) concurrent with the review and update of other project plans, and (5) in preparation for a PD submission.

The project risk management coordinator, if assigned, develops the RMP based on guidance provided by the PD/PM, and coordinating with the IPT. To be effective, the PD/PM must make risk management an important project management function and must be actively involved in the risk planning effort. Planning requires the active participation of essentially the entire PD and contractor team.

6.2.2 Procedures

Figure 8 graphically depicts the process to be followed in applying this technique. The procedure consists of a number of iterative activities that result in the development of the risk management strategy and a RMP.

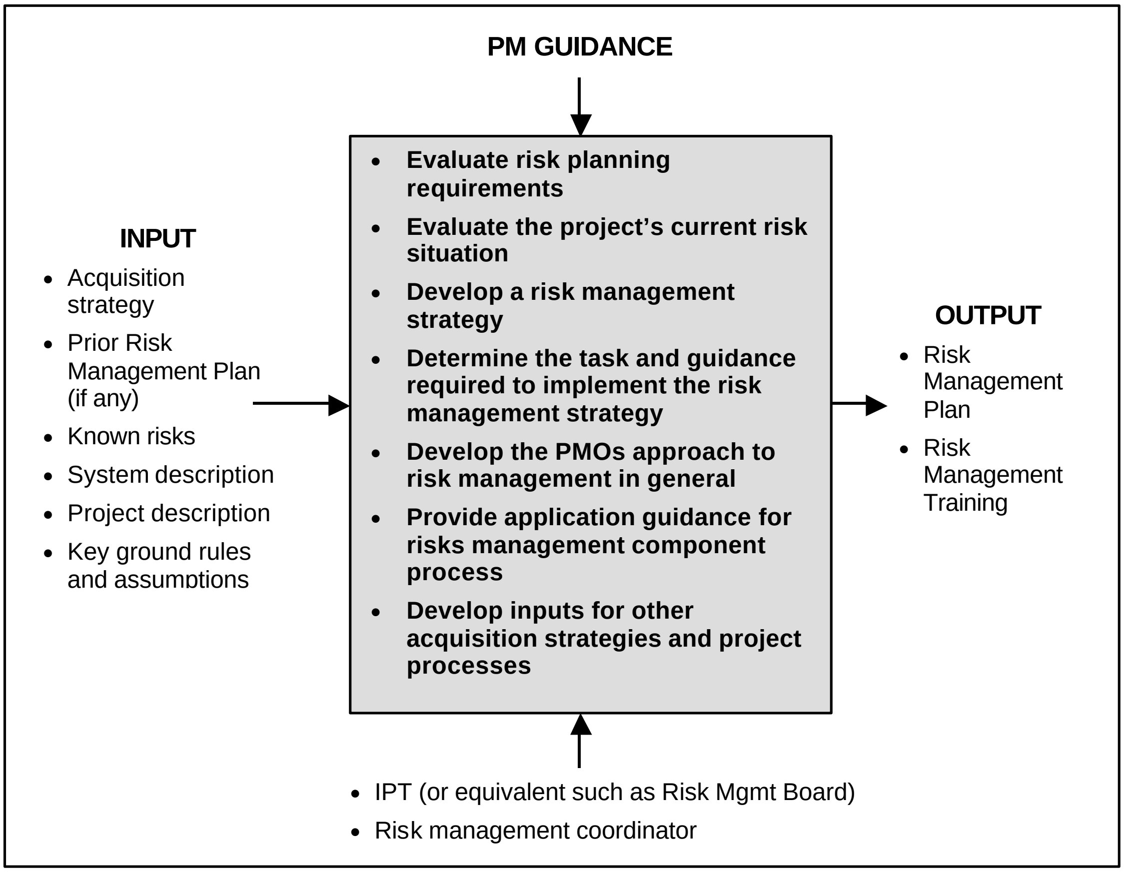


Figure 8. Risk Planning Technique Input and Output

The acquisition strategy and related management planning efforts (project management, and systems engineering), project constraints, and any existing risk management planning are integrated and evaluated in the context of the PD's guidance, which provides the direction for the planning process. Typical types of PD guidance are concerns about certain categories of risk, guidance on funding of handling activities, emphasis to be placed on risk management training, and frequency and type of internal reports.

The integration and evaluation of the primary inputs establish the requirements and scope of the planning effort through an assessment of the project's current risk situation. The results of the assessment provide the basis for development of management strategy. The strategy should reflect the level of risk that the PD/PM is prepared to accept, and should provide guidance on how and when known risks will be reduced to acceptable levels. It should also describe the risk management process the PD/PM will employ and the organization and structure of the management program, addressing things such as risk ratings, the use of a management information system, policy and procedures on sharing risk management information, and training.

The PD/PM should create a management information system early in the planning process. It will serve as a planning source and the data may be used for creating reports. It will also become the repository for all current and historical information related to risk. Eventually, this information may include risk assessment documents, contract deliverables, if appropriate, and other risk-related reports.

Based on the management strategy, the plan identifies specific tasks to be accomplished and assigns responsibility for their execution. The timing of these tasks should be incorporated into an integrated critical path master schedule or equivalent. Guidance for task execution and control should also be developed, covering such things as the suggested techniques to be used for each component, any assistance available to the IPT, the use of funds, the policy on the use of independent risk assessors, etc. This information may be documented in a risk management plan. A sample format is shown in Table 9. Appendix A contains an example of a RMP.

Table 9. Sample Format for a Risk Management Plan

INTRODUCTION. This section should address the purpose and objective of the plan, and provide a brief summary of the project, to include the approach being used to manage the project, and the acquisition strategy.

PROJECT SUMMARY. This section contains a brief description of the project, including the acquisition strategy and the project management approach. The acquisition strategy should address its linkage to the risk management strategy.

DEFINITIONS. Definitions used by the project office should be consistent with DOE definitions for ease of understanding and consistency. However, the DOE definitions allow PDs/PMs flexibility in constructing their risk management programs. Therefore, each program's risk management plan may include definitions that expand DOE definitions to fit its particular needs. For example, each plan should include, among other things, definitions for the ratings used for technical, schedule, and cost risk.

RISK MANAGEMENT STRATEGY AND APPROACH. Provide an overview of the risk management approach, to include the status of the risk management effort to date, and a description of the project risk management strategy.

ORGANIZATION. Describe the risk management organization of the project office and list the responsibilities of each of the risk management participants.

RISK MANAGEMENT PROCESS AND PROCEDURES. Describe the project risk management process to be employed, i.e., risk planning, assessment, handling, monitoring and documentation, and a basic explanation of these components. Also provide application guidance for each of the risk management functions in the process. If possible, the guidance should be as general as possible to allow the project's risk management organization flexibility in managing the project risk, yet specific enough to ensure a common and coordinated approach to risk management. It should address how the information associated with each element of the risk management process will be documented and made available to all participants in the process, and how risks will be tracked to include the identification of specific metrics if possible.

RISK PLANNING. This section describes the risk planning process, provides guidance on how it will be accomplished, and describes the relationship between continuous risk planning and this RMP. Guidance on updates of the RMP and the approval process to be followed should also be included.

RISK ASSESSMENT. This section of the plan describes the assessment (identification and analysis) process. It includes procedures for examining the critical risk areas and processes to identify and document the associated risks. It also summarizes the analyses process for each of the risk areas leading to the determination of a risk rating. This rating is a reflection of the potential impact of the risk in terms of its variance from known best practices or probability of occurrence, its consequence, and its relationship to other risk areas or processes. This section may include:

- Overview and scope of the assessment process
- Information to be reported and formats
- Description of how risk information is retained
- Sources of information
- Assessment techniques and tools

RISK HANDLING. This section describes the risk handling options, and identifies tools that can assist in implementing the risk handling process. It also provides guidance on the use of the various handling options for specific risks.

RISK MONITORING. This section describes the process and procedures that will be followed to monitor the status of the various risk events identified. It should provide criteria for the selection of risks to be reported on, and the frequency of reporting. Guidance on the selection of metrics should also be included.

RISK MANAGEMENT INFORMATION SYSTEM, DOCUMENTATION AND REPORTS. This section describes the management information system structure, rules, and procedures that will be used to document the results of the risk management process. It also identifies the risk management documentation and reports that will be prepared; specifies the format and frequency of the reports; and assigns responsibility for their preparation.

The contents of the risk management strategy and plan should be consistent with the acquisition strategy and other project plans derived from the acquisition strategy. Hence, it should be tailored to each project rather than attempting to use the same process and its implementation for all programs. This will help ensure that risk is considered in all project activities and that it does not become a "stove pipe" function.

6.3 Risk Assessment Techniques

6.3.1 Product (WBS) Risk Assessment

Description. This technique identifies those risks associated with a given system concept and design. The difference between the process (Department of Defense 4245.7-M) technique and this approach is that Department of Defense 4245.7-M addresses the contractor's engineering and manufacturing process and this technique focuses on the resulting product. This technique is used to identify and analyze risks in the following critical areas: design and engineering, logistics, technology, production, concurrency, plus others as needed for both hardware and software.

The WBS is the starting point to describe contract work to be done and the resulting product and is the basis for determining risk events in each critical risk area. The risk events—events that might have a detrimental impact on the system, subsystems, or components—are evaluated to identify and characterize specific risks ratings and prioritization.

This technique should be used shortly after the completion of the prime contractor's WBS. Thereafter, it should be used regularly up to the start of production. The technique can be used independently or in conjunction with other risk assessment techniques, such as the Process (DoD 4245.7-M) Risk Assessment technique. To apply this technique, joint Government and industry evaluation teams should examine the appropriate WBS levels in each product area. If necessary, complementary industry-only teams may take an in-depth look at selected areas at lower WBS levels. At times, it may be desirable to include outside industry experts on the teams to aid in the examination of specific WBS elements or functional areas.

Procedures. Figure 9 depicts the process used in this technique. The first step is to review the WBS elements down to the level being considered, and identify risk events. This review should consider the critical areas (design and engineering, technology, logistics, etc.) that may help to describe risk events. Table 10 provides a partial listing of these elements.

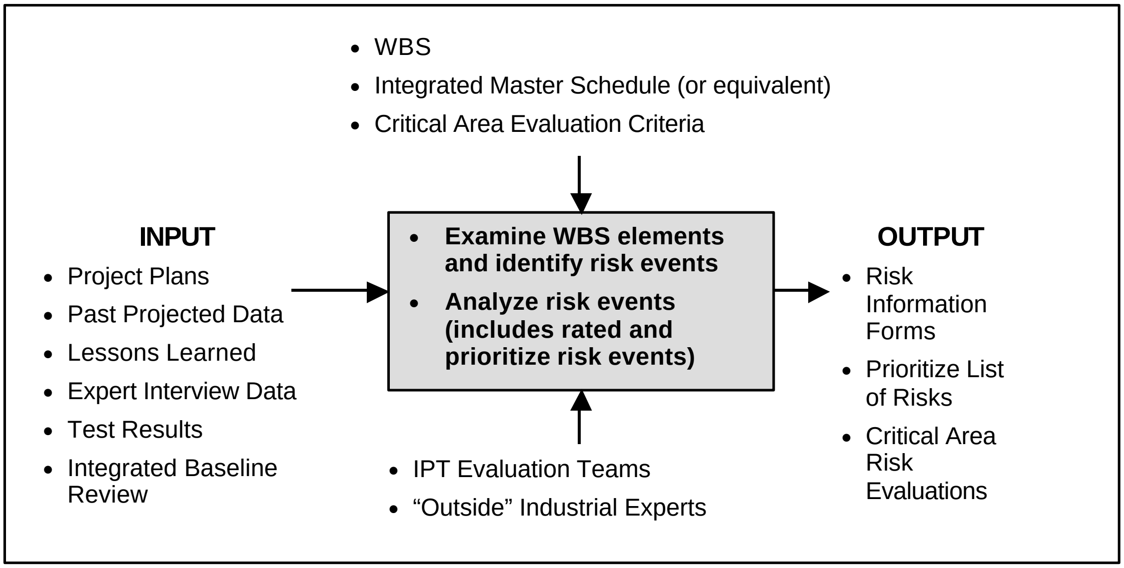


Figure 9. Product (WBS) Risk Assessment Technique Input and Output

Using information from a variety of sources, such as program plans, prior risk assessments, expert interviews, etc., the WBS elements are examined to identify specific risks in each critical area. The risk event, are then analyzed to determine probability of occurrence and consequences/impacts, along with any interdependencies and risk event priorities. Several techniques and tools are available to accomplish this, including, among others, technology assessments, modeling and simulation, hazard analysis, and fault tree analysis.

The results of this analysis should be documented in a project-specific standard format, such as a Risk Information Form. The risks, along with others identified using other techniques, can be prioritized and aggregated using the technique described later in this chapter.

Table 10. Critical Risk Areas and Example Elements

Critical Risk Areas	Example Elements	
Design and Engineering	• Design/technology approach • Operational environments • External/internal interfaces • Use of standard parts/project parts list • System/subsystem critical design requirement	• Integration requirements • Human-machine interface • Design growth capacity • Design maturity • Safety & health hazards • Manpower, training and skill profiles
Logistics	• Operations and Maintenance concept • System diagnostic requirement • Repairability and Maintainability requirements • Supply support requirements • Test requirements	• Support equipment requirements • Maintenance interfaces • Level of repair decisions • Training equipment design
Testing	• Integrated test • Qualification testing • Subsystem test limits	• Test environmental Acceleration • Supportability test results
Manufacturing	• Design producibility • Manufacturing capability requirements • Parts/assemblies availability	• Special tooling/test equipment planning personnel availability • Process/tooling proofing • Production equipment availability
Concurrency	• Program schedule adequacy	• Development phases concurrency

6.3.2 Process Risk Assessment

Description. This technique is used to assess (identify and analyze) project technical risks resulting from the contractor's processes. It is based on the application of the technical risk area templates found in DoD 4245.7-M. These templates describe the risk areas contained in the various technical processes (e.g., design, test, production, etc.) and specify methods for reducing risks in each area. Success of any risk reduction efforts associated with this technique will depend on the contractor's ability and willingness to make a concerted effort to replace any deficient engineering practices and procedures with best industrial practices.

One of the primary benefits of this technique is that it addresses pervasive and important sources of risk in most acquisition programs and uses fundamental engineering principles and proven procedures to reduce technical risks. The technique is accepted by many companies in normal business activities, and in fact, was developed by a group of Government and industry experts.

The technique is primarily applicable during Initiation phase. In the Initiation phase it provides a detailed checklist of processes that the contractor needs to address. The description of each template in DoD 4245.7-M shows the phases in which the template should be applied. The specific timing of the application within the phases should be determined based on the type of project, the acquisition strategy and plans, and the judgment of project officials. It should also be used in preparation for milestone decisions and when preparing for source selection. This technique may be used independently or in conjunction with other risk assessment techniques.

When feasible, a Government-industry evaluation team should be formed early in the program to apply this technique.

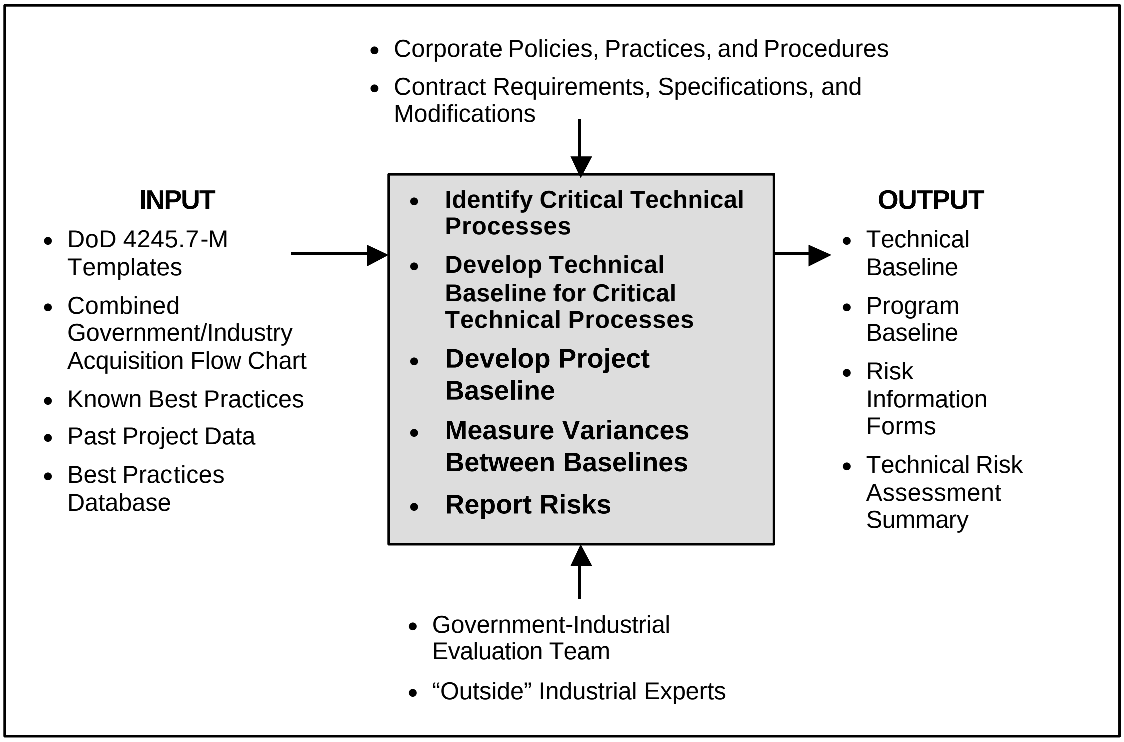


Figure 10. Process Risk Assessment Technique Input and Output

Procedures. Figure 10 shows the basic approach used in this technique. The DoD 4245.7-M templates are used in conjunction with the contract requirements and specifications to identify those technical processes critical to the project and to establish a project baseline of contractor processes. When possible, the project baseline should be determined by evaluating actual contractor performance, as opposed to stated policy. For example, design policy should be determined from interviewing designers and not simply from reviewing written corporate policies.

This project baseline should then be compared to a baseline of industry-wide processes and practices that are critical to the project. The baseline should be developed by reviewing and compiling known best practices in use by various companies in both defense and non-defense sectors. The point of contact for the DoD Best Manufacturing Practices Center of Excellence can be found at: http://www.bmpcoe.org.

The differences between the two baselines are a reflection of the technical process risk present. These results should be documented in a standard format, such as a project-specific Risk Information Form (see management information system discussion in this section) to facilitate the development of a risk-handling and risk-reporting plan.

6.3.3 Program Documentation Evaluation Risk Identification

Description. This technique provides a methodology for comparing key program documents and plans to ensure that they are consistent and traceable to one another. Project documents and plans are hierarchical in nature. If the contents (activities, events, schedules, requirements, specifications, etc.) of a document or plan do not flow from or support the contents of those above, below, or adjacent to it, there is a strong chance that risk will be introduced into the project or that known risks will not be adequately addressed. This technique reduces those risks and improves the quality of program documentation.

This technique can be used in any acquisition phase as documents or plans are being developed or updated. The comparison of program documentation and plans should be performed by a small team of experienced, knowledgeable personnel who are intimately familiar with the total project.

Procedures. Figure 11 shows the process used in this technique. The primary inputs to the process are the project documents that detail the steps involved in executing the program. These include, for example, the Mission Need Statement (MNS), acquisition plan, any master management plan, test and plans, manufacturing plan, etc. Another set of key input documents are those used to communicate with the contractor, e.g., WBS, specifications, Statement of Work or equivalent such as Statement of Objectives, etc. Before any comparison, the PD/PM should review all documents for accuracy and completeness. Figure 12 shows an example of the type of correlation that should exist between the MNS, requirements document, and test place during the Initiation phase. If the comparison shows any gaps or inconsistencies, reviewers should identify them as possible risks on a Risk Identification Form, the output of this process.

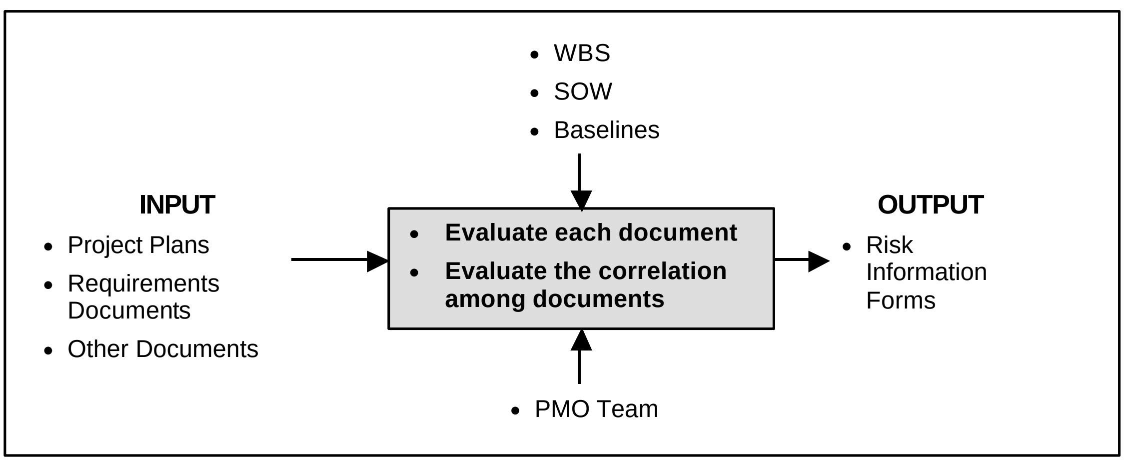


Figure 11. Plan Evaluation Technique Input and Output

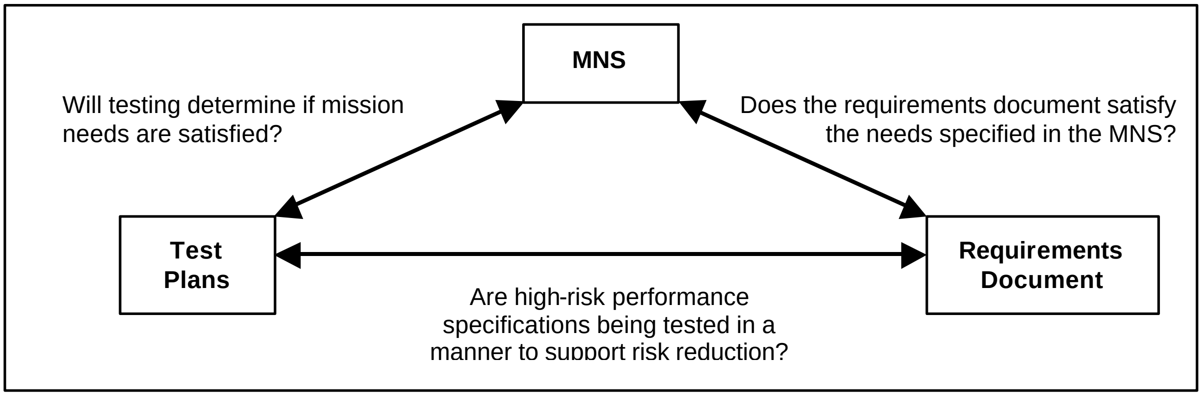


Figure 12. Initiation Phase Correlation of Selected Documents (Example)

6.3.4 Threat and Requirements Risk Assessment

Description. This technique describes an approach to assess risks associated with requirements and threat and to identify requirements and threat elements that are risk drivers. Because operational needs, environmental demands, and threat determine system performance requirements, to a large degree, they are a major factor in driving the design of the system and can introduce risk in a program. The requirements risk assessment process focuses on: determining if operational requirements are properly established and clearly stated for each program phase; ensuring that requirements are stable and the operating environment is adequately described; addressing logistics and suitability needs; and determining if requirements are too constrictive, thereby identifying a specific solution. The evaluation of the threat risk assessment process' maturity addresses: uncertainty in threat accuracy and stability, sensitivity of design and technology to threat, vulnerability of the system to threat counter-measures, and vulnerability of the project to intelligence penetration. PD/PMs should view requirements in the context of the threat and accurately reflect operational, environmental, and suitability requirements in design documents.

PD/PMs should use threat and requirements assessments during the early phases of project development and, as necessary, as the project advances through development. Early and complete understanding of the requirements and threat precludes misunderstandings between the requirements and development communities, helps to identify risk areas, and allows early planning to handle risk. Consequently, the user should be actively involved in this process from the beginning.

Procedures. Figure 14 depicts the process used in this technique. The basic approach is to conduct a thorough review of the documents containing performance requirements and threat information to determine stability, accuracy, operating environment, logistics and suitability requirements, and consistency between these requirements and the threat considerations cited above. There should be an understanding between the users and the developers on Key Parameters (KPs) in order to identify the requirements that are most important and critical to project success. The Design Reference Mission Profile and Design Requirements templates in DoD 4245.7-M and the Program Documentation Evaluation Risk Identification technique may be useful in support of this technique.

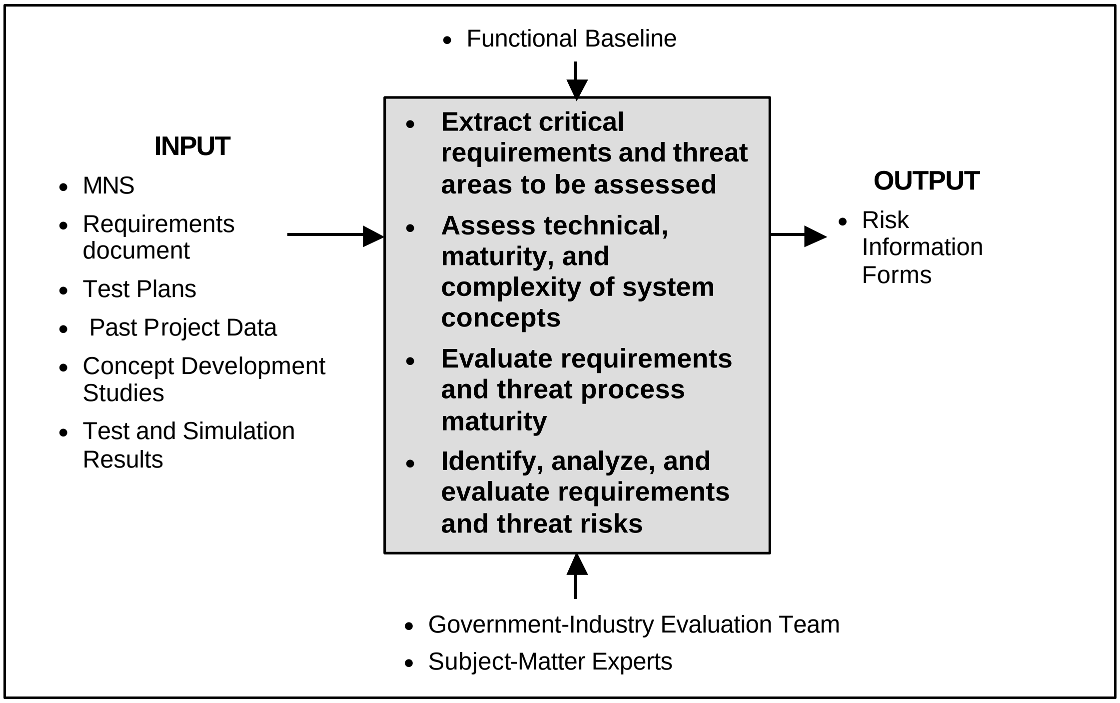


Figure 14. Threat and Requirement Risk Assessment Technique Input and Output

Requirements should be thoroughly reviewed to identify those that drive performance. This will require the "flow down" of performance requirements to components and subassemblies and the identification of technologies/techniques to be used in these components/ subassemblies that may significantly affect the system's ability to meet users' needs.

Designers should determine the sensitivity of system performance to the requirements and threat and identify risk drivers. Models and simulations are useful tools to determine this sensitivity. For example, the U.S. Army Materiel System Analysis Activity has such an analytic model, the Army Materiel System Analysis Activity Risk Assessment Methodology.

6.3.5 Cost Risk Assessment

Description. This technique provides a project-level cost estimate at completion (EAC) that is a function of performance (technical), and schedule risks. It uses the results of previous assessments of WBS elements and cost probability distributions developed for each of the elements. These individual WBS elements are aggregated using a Monte Carlo simulation to obtain a probability distribution of the program-level cost EAC probability distribution function. These results are then analyzed to determine the actual risk of cost overruns and to identify the cost drivers.

The use of these cost probability distributions as the basis for the program-level cost estimate results in a more realistic EAC than the commonly used single point estimates for WBS elements, since they address both the probability of occurrence and consequences/impacts of potential risks. Their use eliminates a major cause of underestimating (use of point estimates) and permits the evaluation of performance (technical) or schedule causes of cost risk. Thus, this technique provides a basis for the determination of an “acceptable” level of cost risk.

This technique can be used in any of the acquisition phases, preferably at least once per phase beginning in the Initiation phase although suitable data may not exist until the Definition phase in some cases. It should be used in conjunction with performance (technical) and schedule risk assessments and may be performed by small Government-industry teams consisting of risk analysts, cost analysts, schedule analysts and technical experts who understand the significance of previous performance and schedule risk assessments. They should report to the IPT. This technique requires close and continuous cooperation among cost analysts and knowledgeable technical personnel and the support of the contractor’s senior management to help get valid cost data.

Procedures. Figure 15 depicts the process used in applying this technique. The first step is to identify the lowest WBS level for which cost probability distribution will be constructed. The level selected will depend on the project phase; e.g., Initiation, may not be possible to go beyond level-2 or -3, simply because the WBS has not yet been developed to lower levels. As the project advances into subsequent phases and the WBS is expanded, it will be possible and necessary to go to lower levels (4, 5, or lower). Specific performance (technical) and schedule risks are then identified for these WBS elements.

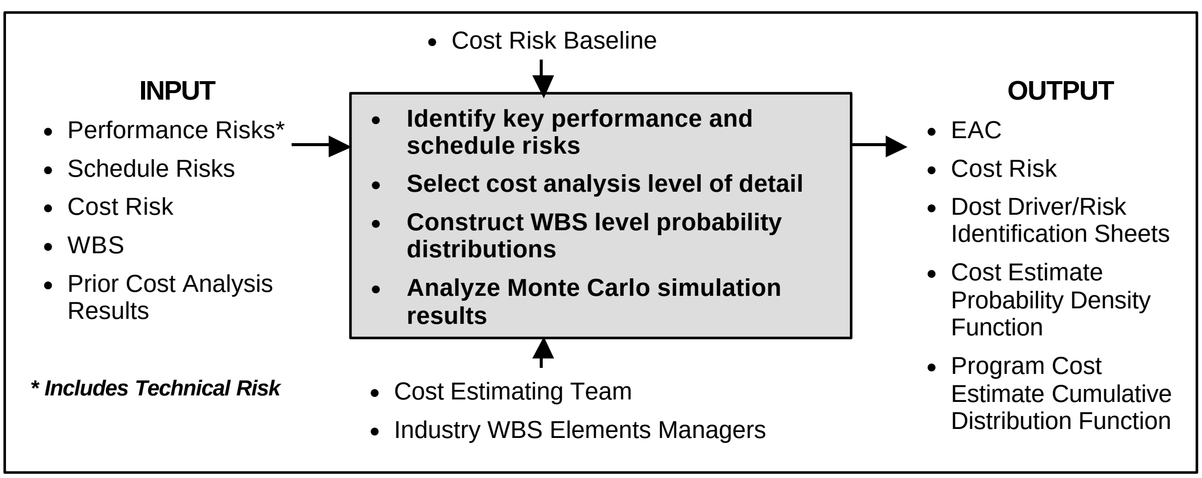


Figure 15. Cost Risk Assessment Top-Level Diagram

To develop the WBS elements cost probability distributions, the team, working with the contractor’s WBS element managers, determines the cost range for each element being investigated. The cost range encompasses cost estimating uncertainty, schedule risk, and technical risk. The validity of the cost data used to construct the distribution is critical. In fact, collecting good data is the largest part of the cost risk job. Consequently, PDs/PMs should place major emphasis on this effort.

The element cost probability distributions are aggregated and evaluated using a Monte Carlo simulation program. All Monte Carlo processes contain limitations, but they are more informative than point estimates. Any number of these simulations are readily available to perform this aggregation, and one that meets the specific needs of the program should be selected. The results of this step will be a program-level cost EAC and a cost distribution that shows the cumulative probability associated with different cost values. These outputs are then analyzed to determine the level of cost risk and to identify the specific cost drivers. Cost risk is determined by comparing the EAC with the cost baseline developed as part of the PB. Since the EAC and program cost distribution are developed from WBS element risk assessments, it is possible to determine the cost risk drivers. The cost drivers can also be related back to the appropriate performance and schedule risks. The results of the analysis (cost risks and drivers) should be documented in risk identification forms.

6.3.6 Quantified Schedule Risk Assessment

Description. This technique provides a means to determine program-level schedule risk as a function of risk associated with various activities that compose the program. It estimates the project-level schedule by developing probability distributions for each activity duration and aggregating these distributions using a Monte Carlo simulation or other analytical tools. The resulting program-level schedule is then analyzed to determine the actual schedule risk and to identify the schedule drivers.

This technique expands the commonly used Critical Path Method of developing a project schedule to obtain a realistic estimate of schedule risk. The basic Critical Path Method approach uses single point estimates for the duration of program activities to develop the project's expected duration and schedule. It invariably leads to underestimating the time required to complete the project and schedule overruns, primarily because the point estimates do not adequately address the uncertainty inherent in individual activities.

The quantified schedule technique accounts for uncertainty by using a range of time that it will take to complete each activity instead of single point estimates. These ranges are then combined to determine the project-level schedule estimate. This approach enables PDs/PMs to estimate early in a project if there is a significant probability/likelihood of overrunning the program schedule and by how much. It also identifies program activities that are on the "highest risk path."

This technique can be used in any acquisition phase beginning with the completion of the first statement of work. The schedule probability distribution function for each key activity should be developed as soon as the activity is included in the master schedule. The distribution functions should be periodically reviewed and revised, if necessary, at least once per phase. The technique should be applied by a small Government-industry team consisting of schedule analysts and technical experts who understand the significance of prior risk performance assessments.

Procedures. Figure 16 shows the process used in this technique. The first step is to identify the lowest activity level for which duration/schedule probability distribution functions will be constructed. The WBS should be used as the starting point for identifying activities and constructing a network of activities. The WBS level selected will depend on the project phase.

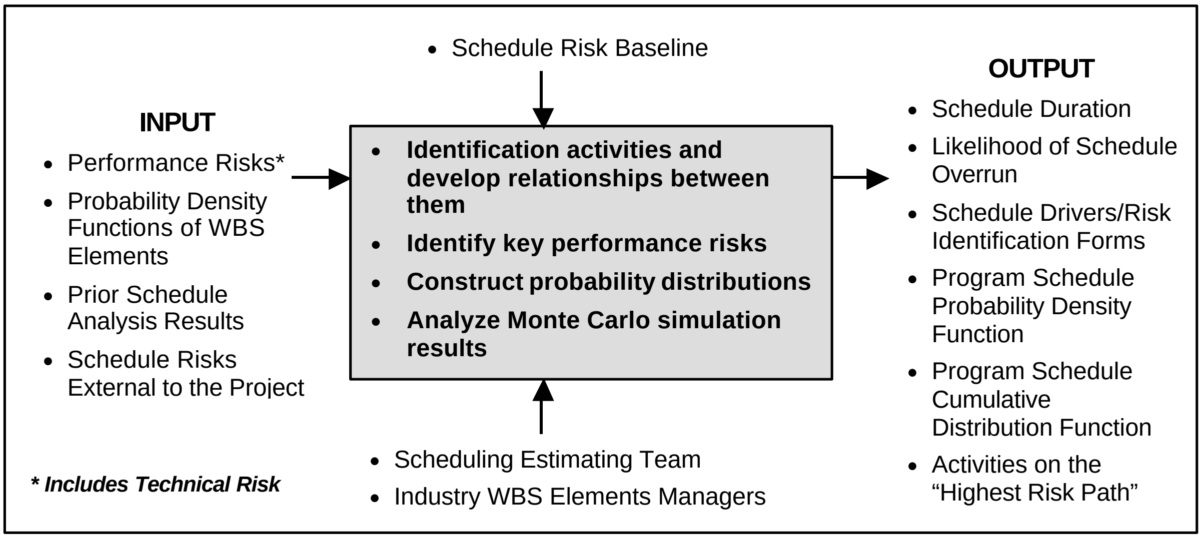


Figure 16. Schedule Risk Assessment Technique Input and Output

Next, the contractor should construct a Critical Path Method schedule for these activities. To develop the activity duration probability distribution functions, the team, working with the prime contractor's WBS element managers, determines and analyzes duration range for each activity being investigated. Schedule analysts working closely with knowledgeable technical people should perform this analysis.

The activity duration probability distributions are aggregated using a Monte Carlo simulation program, such as ©Risk, Risk + for Microsoft® Project, or Crystal Ball. The result of this step is a project-level schedule and distribution function that shows the cumulative probability associated with different duration values. These outputs are then analyzed to determine the level of schedule risk and to identify the specific schedule drivers. Risk is determined by comparing the project-level schedule with the deterministic schedule baseline developed as part of the PB. The fact that the schedule and distribution are developed from WBS element risk assessments makes it possible to determine the schedule risk drivers. These drivers can also be related back to the appropriate performance risks. The results of the analysis (schedule risks and drivers) should be documented in Risk Information Forms. The analysis requires continued close cooperation between the schedule analysts and technical personnel familiar with the details of the project.

6.3.7 Expert Interviews

Description. A difficult part of the risk management process is data gathering. This technique provides a means for collecting risk-related data from subject-matter experts and from people who are intimately involved with the various aspects of the project. It relies on “expert” judgment to identify and analyze risk events, develop alternatives, and provide “analyzed” data. It is used almost exclusively in a support role to help develop technical data, such as probability and consequences/impacts information, required by a primary risk assessment technique. It can address all the functional areas that make up the critical risk areas and processes, and can be used in support of risk handling. Expert judgment is a sound and practical way of obtaining necessary information that is not available elsewhere or practical to develop using engineering or scientific techniques. However, interviewers should be aware that expert opinions may be biased because of over-reliance on certain information and neglect of other information; unwarranted confidence; the tendency to recall most frequent and most recent events; a tendency to neglect rare events; and motivation. Results may have to be tempered because of these biases.

Procedures. Figure 17 depicts the process used in this technique. The first step in the process is to identify risk areas and processes that are to be evaluated using the expert interview technique. Other techniques described in this section (e.g., WBS Risk Assessment, Process Risk Assessment, etc.) can be used for this purpose.

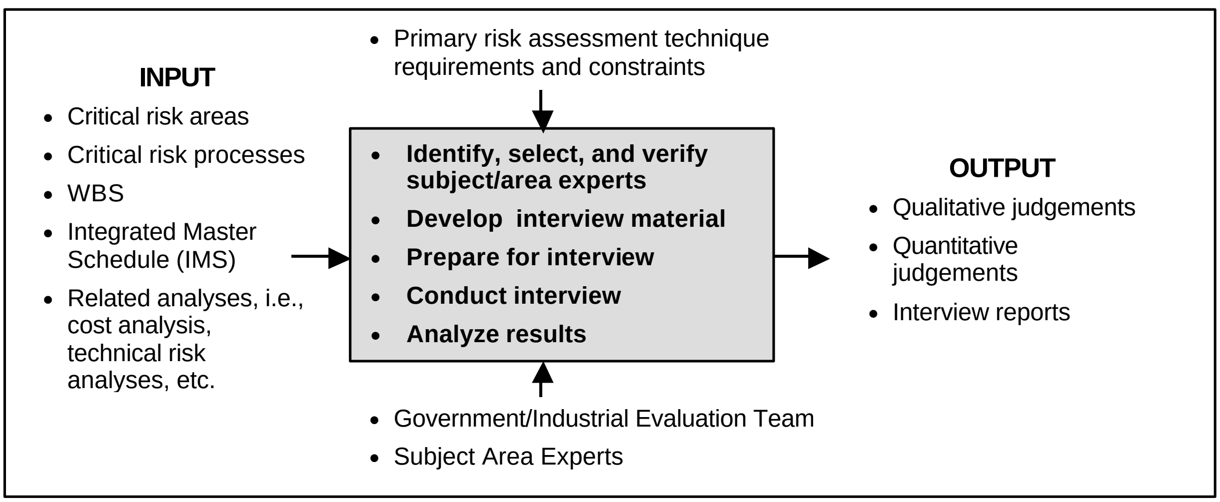


Figure 17. -Expert Interview Technique Input and Output

Once the areas and processes are known, subject-matter experts and project/contractor personnel knowledgeable of the areas and processes should be identified to be interviewed. Similarly, qualified interviewers should be selected for each area and process.

Interviewers should prepare themselves by preparing a strategy and selecting a methodology for analysis and quantification of data. The references list sources for practical techniques for quantifying expert judgment.

After the interview, evaluators analyze the data for consistency, resolve any issues, and document the results. Commercial "groupware" software is available to assist in compiling and documenting the results of interviews.

6.3.8 Analogy Comparison/Lessons-Learned Studies

Description. This technique uses lessons learned and historical information about the risk associated with projects that are similar to the new system to identify the risk associated with a new project. It is normally used to support other primary risk assessment techniques, e.g., Product (WBS) Risk Assessment, Process Risk Assessment, etc. The technique is based upon the concept that "new" projects are originated or evolved from existing projects or simply represents a new combination of existing components or subsystems. This technique is most appropriate when systems engineering and systems integration issues, plus software development, are minimal. A logical extension of this premise is that key insights can be gained concerning aspects of a current project's risks by examining the successes, failures, problems, and solutions of similar existing or past projects. This technique addresses all the functional areas that make up the critical risk areas and processes.

Procedures. Figure 18 depicts the process used in this technique. The first step in this approach is to select or develop a Baseline Comparison System that closely approximates the characteristics of the new system/equipment to as low a level as possible and uses the processes similar to those that are needed to develop the new system. For processes, industry-wide best practices should be used as a baseline.

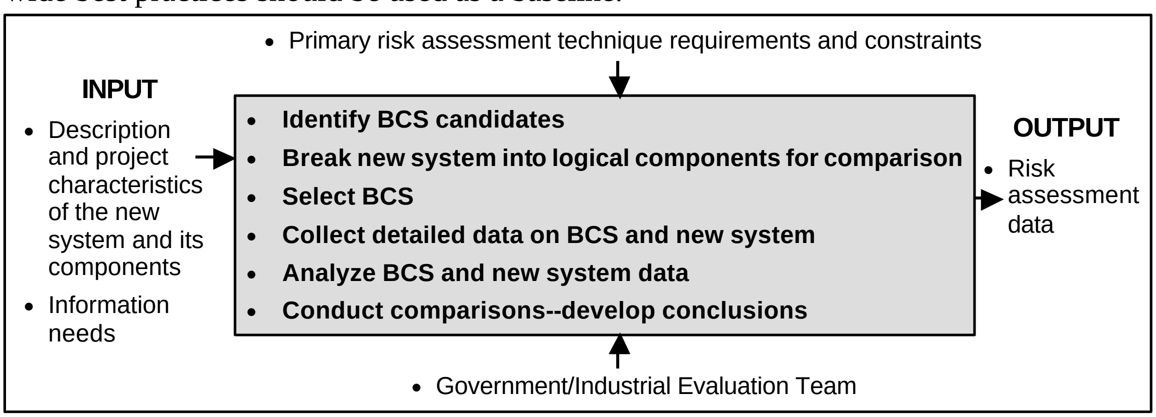


Figure 18. Analogy Comparison/Lessons Learned Studies Top-Level Diagram

Relevant baseline comparison system data are then collected, analyzed, and compared with the new system requirements. The baseline comparison system data may require adjustment to make a valid comparison; for example, apply appropriate inflation indices for cost comparisons, adjust design schedule for software evolution versus software development, etc. The comparisons can be a major source of risk assessment data and provide some indication of areas that should be investigated further.

6.4 Risk Prioritization

6.4.1 Description

This technique provides a means to prioritize the risks present in a project. It is a part of risk analysis. The prioritized list provides the basis for developing handling plans, preparing a handling task sequence list, and allocating handling resources.

When using this technique, PDs/PMs establish definitive criteria to evaluate the risks, such as, probability (probability/likelihood) of failure, (P_F), and consequence/impact of failure (C_F), along with any other factors considered appropriate. The risks are evaluated using qualitative expert judgment and multi-voting methods to prioritize and aggregate risks. (See References—*SEI, Continuous Risk Management*, 1996, for a discussion of multi-voting methods.)

A qualitative approach using subject-matter experts is generally preferred in this technique because of the tendency to rely on ordinal values to describe P_F, C_F and the inherent inaccuracies resulting from any attempts to use quantifiable methods derived from raw (uncalibrated) ordinal scales.

This technique should be used appropriately during the Initiation phase, at the conclusion of a major risk assessment undertaking, when there has been a significant change in the acquisition strategy, when risk monitoring indicates significant changes in the status of a number of risks, and prior to a milestone review.

The project risk management coordinator (if assigned) may function as a facilitator and support the project IPT in applying this technique.

6.4.2 Procedures

Figure 19 depicts the process used to prioritize the risks present in a program. The inputs of this process are risks that have been identified.

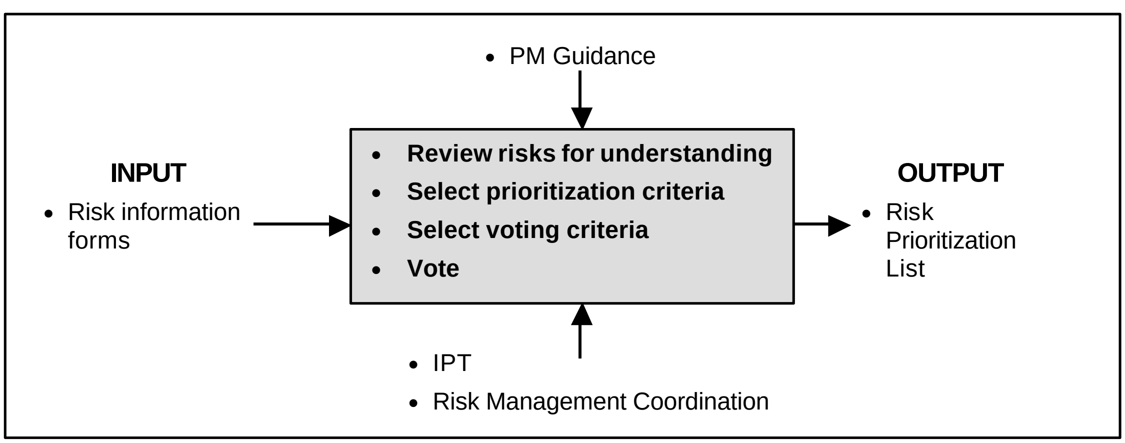


Figure 19. Risk Prioritization Technique Input and Output

The evaluation team, through consensus or as directed by the RMP, selects the prioritization criteria. P_F and C_F should always be part of the criteria, along with any other appropriate factors. Urgency, an indication of the time available before the procedures for handling the specific risk must be initiated, is often considered in the evaluation. The PD/PM may also choose to rank-order the prioritization criteria, e.g., consequence/impact is more important than probability.

A multi-voting method is useful to prioritize risks (see References-Scholtes, 1988; Linstone, 1975). The Delphi method is a simple and effective method of arriving at a consensus among a group of experts. The procedure is for team members to vote on the priority of each risk and tally the results, which are fed back to the team. Team members vote again and the process is repeated until no changes occur in the results. It is normal to reach the final outcome within a few voting sessions. If there are a large number of risks, they may be broken into smaller groups for ranking. As a general rule, no more than 10 items should be prioritized per vote. The results of the series of votes are documented in the risk prioritization list.

PD/PM guidance, which operates as a technique control function, can be used, for example, to specify prioritization criteria and prescribe the format of the risk prioritization list.

Risk Aggregation. Figure 20 shows the process for this technique, which relies on qualitative judgment and multi-voting methods to summarize risks at the critical risk area and process level in terms of P_F and C_F. The risks identified in the Risk Identification Forms and Risk Prioritization List are first grouped according to critical risk areas and processes, and listed in priority sequence.

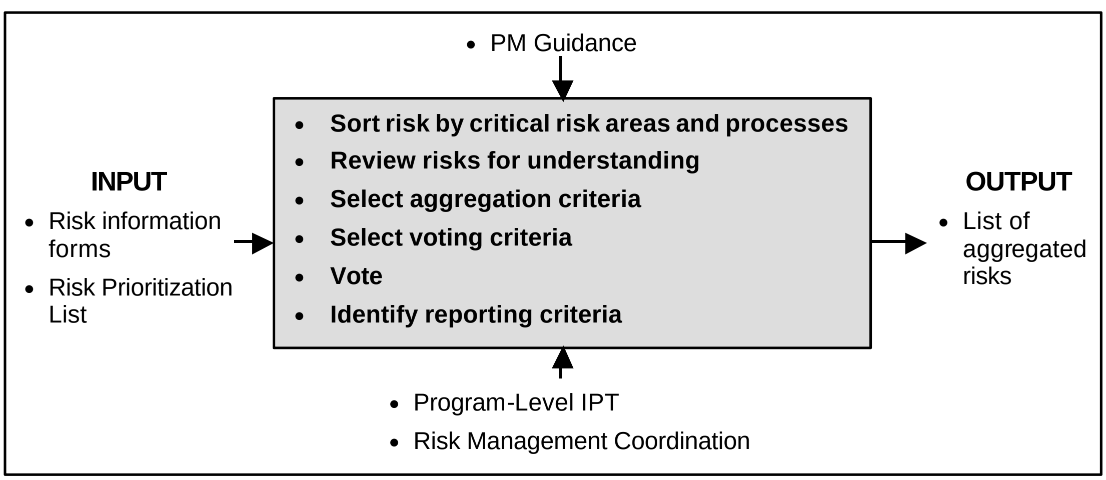
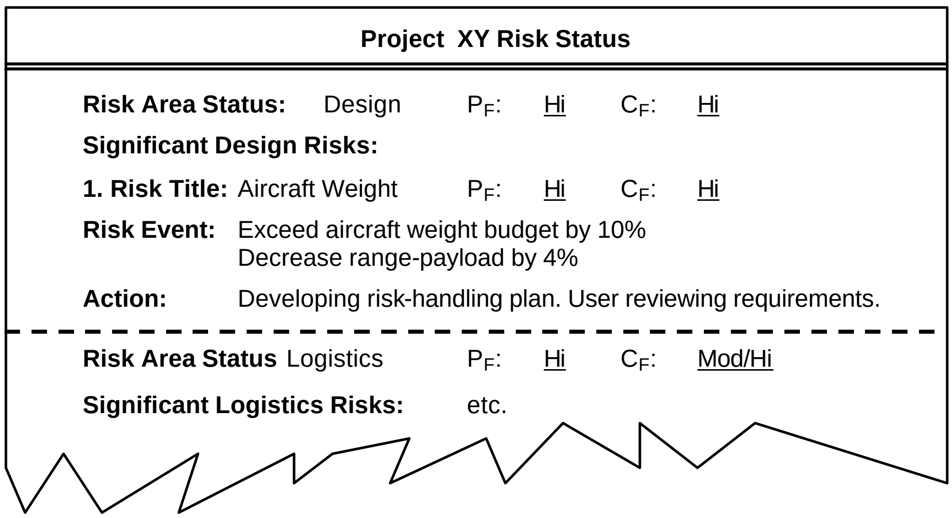


Figure 20. Risk Aggregation Technique Input and Output

Within each area and process, individual risks are evaluated against a set of established criteria to determine the overall aggregate risk rating for the area/process. Aggregation criteria is to be established separately for P_F and C_F; P_F and C_F should not be combined into a single index, e.g., moderate risk. Examples of aggregation criteria include: (1) most undesirable P_F and C_F of all the risks within a risk area or process becomes the aggregated values for the area or process, or (2) the P_F and C_F for each area or process represents the mean value for that area or process.

The team then votes on each risk area and process to determine its rating for P_F and C_F, and documents the results. In addition to the P_F and C_F ratings for each critical risk area and process, those risks that tend to "drive" the aggregate risk rating for the area/process should be included in a list of aggregated risks to give substance to the aggregated ratings, e.g., all risks where either P_F or C_F are rated as high. Figure 21 provides a sample list of aggregated risks.



Project XY Risk Status

Risk Area Status: Design P_F: Hi C_F: Hi

Significant Design Risks:

1. Risk Title: Aircraft Weight P_F: Hi C_F: Hi

Risk Event: Exceed aircraft weight budget by 10%
Decrease range-payload by 4%

Action: Developing risk-handling plan. User reviewing requirements.

Risk Area Status Logistics P_F: Hi C_F: Mod/Hi

Significant Logistics Risks: etc.

Figure 21. Sample of a List of Prioritized Risks

Risk Matrix is a software tool that is designed to aid in managing the identification, rating, and prioritization of key risks that might affect a project. It provides a structured method for prioritizing project risks and for tracking the status and effects of risk-handling efforts. The major feature that Risk Matrix offers the project office is a means to both rate and rank project risks. This is helpful in differentiating among risks that have the same rating. For example, if a project has eight risks that the project office has evaluated/rated as high, Risk Matrix provides the means to rank them in order of severity. The user can use this ranking as a guide to help focus risk-handling efforts. Risk Matrix was developed by the Air Force Electronic Systems Center and The Mitre Corporation and may be available to project offices free of charge. Another useful software tool to use in voting on risks is "Expert Choice"--based on the Analytical Hierarchy Process. Whatever software tool is used, the analyst should recognize that a number of inherent limitation exist with such software tools, (e.g., unintentionally biasing the voting process) that can lead to erroneous results.

6.5 Risk-Handling Techniques

6.5.1 General (e.g., Moderate and High Risk-Rated Items)

After the project's risks have been assessed, the PD/PM must develop approaches to handle significant ones by analyzing various handling techniques and selecting those best fitted to the project's circumstances. The PD/PM should reflect these approaches in the project's acquisition strategy and include the specifics on what is to be done to deal with the risk, when it should be accomplished, who is responsible, and the cost and schedule impact.

As described previously, there are essentially four risk-handling techniques, or options. Risk avoidance eliminates the sources of high risk and replaces them with a lower-risk solution. Risk transfer is the reallocation of risk from one part of the system to another, or the reallocation of risks between the Government and the contractor or within Government agencies. Risk control manages the risk in a manner that reduces the probability/likelihood of its occurrence and/or minimizes the risk's effect on the project. Risk assumption is the acknowledgment of the existence of a particular risk situation and a conscious decision to accept the associated level of risk without engaging in any special efforts to control it. There is a tendency on many projects to select "control" as the risk-handling option without seriously evaluating assumption, avoidance, and transfer. This is unwise, since control may not be the best option, or even appropriate option in some cases. An unbiased assessment of risk-handling options should be performed to determine the most appropriate option.

In determining the "best" overall risk-handling strategy and specific techniques to be adopted, the following general procedures apply.

For each evaluated event risk, all potentially applicable techniques should be identified and evaluated, using the following criteria:

- Provides project cost excursions from:
  - — Near-term budget execution impacts,
  - — External budget changes and constraints.
- ***Feasibility.*** Feasibility is the ability to implement the handling technique and includes an evaluation of the potential impact of the technique in the following areas:
  - — Technical considerations, such as testing, manufacturing, and maintainability, caused by design changes resulting from risk-handling techniques.
  - — Adequacy of budget and schedule flexibility to apply the technique.
  - — Operational issues such as usability (man-machine interfaces), transportability, and mobility.
  - — Organizational and resource considerations, e.g., manpower, training, and structure.
  - — Environmental issues, such as the use of hazardous materials to reduce technical risk.

— External considerations beyond the immediate scope of the program, such as the impact on other complementary systems or organizations.

- ***Cost and schedule implications.*** The risk-handling techniques have a broad range of cost implications in terms of dollars, as well as other limited resources, e.g., critical materials and national test facilities. The magnitude of the cost and schedule implications will depend on circumstances and can be assessed using such techniques as cost-benefit analyses and the cost and schedule assessment techniques previously described. The approval and funding of risk-handling techniques should be part of the trade-off process that establishes and refines the project's cost and performance goals.
- ***Effect on the system's technical performance.*** The risk-handling techniques may affect the system's capability to achieve the required technical performance objectives. This impact must be clearly understood before adopting a specific technique. As the risk-handling techniques are assessed, the PD/PM should attempt to identify any additional parameters that may become critical to technical performance as a result of implementing them. Trade studies and sensitivity analyses can be useful in determining the expected effectiveness of this approach.

Once the risk-handling technique is selected, a set of project management indicators should be developed to provide feedback on project progress, effectiveness of the risk-handling options selected, and information necessary to manage the project. These indicators should consist of cost and scheduling data, technical performance measures, and project metrics.

Subsequent paragraphs in this section describe the various risk-handling techniques cited above.

6.5.2 Risk Control

Description. In this risk-handling technique, the Government and contractor take active steps to reduce the probability/likelihood of a risk event occurring and to reduce the potential impact on the project. Most risk-control steps share two features: they require a commitment of project resources, and they may require additional time to accomplish them. Thus, the selection of risk-control actions will undoubtedly require some tradeoff between resources and the expected benefit of the actions. Some of the many risk-control actions include the following:

Multiple Development Efforts. The use of two or more independent design teams (usually two separate contractors, although it could also be done internally) to create competing systems in parallel that meet the same performance requirements.

Alternative Design. Sometimes, a design option may include several risky approaches, of which one or more must come to fruition to meet system requirements. However, if the PD/PM studies the risky approaches, it may be possible to discover a lower-risk approach (with a lower performance capability). These lower-risk approaches could be used as backups for those cases where the primary approach(es) fail to mature in time. This option presumes there is some trading room among requirements. Close coordination between the developer and the user is necessary to implement lower capability options.

Trade Studies. Systems engineering decision analysis methods include trade studies to solve a complex design problem. The purpose of the trade studies is to integrate and balance all engineering requirements in the design of a system. A properly done trade study considers risks associated with alternatives.

Early Prototyping. The nature of a risk can be evaluated by a prototype of a system (or its critical elements) built and tested early in the system development. The results of the prototype can be factored into the design and manufacturing process requirements. In addition to full-up systems, prototyping is very useful in software development and in determining a system’s man-machine interface needs. The key to making prototyping successful as a risk-control tool is to minimize the addition of new requirements to the system after the prototype has been tested (i.e., requirement changes not derived from experience with the prototype). Also, the temptation to use the prototype design and software without doing the necessary follow-on design and coding/manufacturing analyses should be avoided.

Incremental Development. Incremental development is completion of the system design and deployment in steps, relying on pre-planned product improvements or software improvements after the system is deployed to achieve the final system capability. Usually, these added capabilities are not included originally because of the high risk that they will not be ready along with the remainder of the system. Hence, development is split, with the high-risk portion given more time to mature. The basic system, however, incorporates the provisions necessary to include the add-on capabilities. Incremental development of the initial system requirements is achieved by the basic system.

Technology Maturation Efforts. Technology maturation is an off-line development effort to bring an element of technology to the necessary level so that it can be successfully incorporated into the system (usually done as part of the technology transition process). Normally, technology maturation is used when the desired technology will replace an existing technology. In those cases, technology maturation efforts are used in conjunction with pre-planned product improvement efforts. However, it can also be used when a critical, but immature, technology is needed. In addition to dedicated efforts conducted by the PD/PM, Service or DOE-wide technology improvement programs and advanced technology demonstrations by Government laboratories as well as industry should be considered.

Robust Design. This approach uses advanced design and manufacturing techniques that promote achieving quality through design. It normally results in products with little sensitivity to variations in the manufacturing process.

Reviews, Walk-Throughs, and Inspections. These three risk control actions can be used to reduce the probability/likelihood and potential consequences/impacts of risks through timely assessments of actual or planned events in the development of the product. They vary in the degree of formality, level of participants, and timing.

Reviews are formal sessions held to assess the status of the program, the adequacy and sufficiency of completed events, and the intentions and consistency of future events. Reviews are usually held at the completion of a project phase, when significant products are available. The team conducting the review should have a set of objectives and specific issues to be addressed. The results should be documented in the form of action items to be implemented by the PD/PM . The type of review will dictate the composition of the review team, which may include developers, users, managers, and outside experts.

A walk through is a technique that can be very useful in assessing the progress in the development of high or moderate risk components, especially software modules. It is less formal than a review, but no less rigorous. The person responsible for the development of the component "walks through" the product development (to include perceptions of what is to be done, how it will be accomplished, and the schedule) with a team of subject-matter experts. The team reviews and evaluates the progress and plans for developing the product and provides immediate and less formal feedback to the responsible person, thus enabling improvements or corrective actions to be made while the product is still under development. This technique is applied during the development phases, as opposed to reviews, which are normally held at the completion of a phase or product.

Inspections are conducted to evaluate the correctness of the product under development in terms of its design, implementation, test plans, and test results. They are more formal and rigorous than either reviews or walk throughs and are conducted by a team of experts following a very focused set of questions concerning all aspects of the product.

Design of Experiments. This is an engineering tool that identifies critical design factors that are difficult to meet.

Open Systems. This approach involves the use of widely accepted commercial specifications and standards for selected system interfaces, products, practices, and tools. It can provide reduced life cycle costs, improved performance, and enhanced interoperability, especially for long life systems with short-life technologies. Properly selected and applied commercial specifications and standards can result in lower risk through increased design flexibility; reduced design time; more predictable performance; and easier product integration, support, and upgrade. However, a number of challenges and risks are associated with the use of the open systems approach and must be considered before implementation. These include such issues as: maturity and acceptability of the standard and its adequacy for use, loss of control over the development of products used in the system, amount of product testing done to ensure conformance to standards, and the higher configuration management workload required.

Use of Standard Items/Software Reuse. The use of standard items and software module reuse should be emphasized to the extent possible to minimize development risk. Standard items range from components and assemblies to full-up systems. A careful examination of the proposed system option will often find more opportunities for the use of standard items or existing software modules than first considered. Even when the system must achieve previously unprecedented requirements, standard items can find uses. A strong program policy emphasizing the use of standard items and software reuse is often the key to taking advantage of this source of risk control. Standard items and software modules have proven characteristics that can reduce risk. However, the PD/PM must be cautious when using standard items in environments and applications for which they were not designed. A misapplied standard item often leads to problems and failure. Similarly, if the cycle for a fielded product extends for many years, it is possible that key software tools and products will become obsolete or will no longer be supported. If this occurs, costly redesign may result if software redevelopment is necessary.

Two-Phase Development. This risk control approach incorporates a formal risk-reduction effort in the initial part of the initiation or development phase. It may involve using two or more contractors with a down-select occurring at a predefined time (normally after the preliminary design review). A logical extension of this concept is the "spiral" development model, which emphasizes the evaluation of alternatives and risk assessments throughout the system's development and initial fielding.

Use of Mockups. The use of mockups, especially man-machine interface mock-ups, can be used to conduct early exploration of design options. They can assist in resolving design uncertainties and providing users with early views of the final system configuration.

Modeling/Simulation. The use of modeling and simulation can provide insight into a system's performance and effectiveness sensitivities. Decision-makers can use performance predictions to assess a system's worth not only before any physical prototypes are built, but also throughout the system life cycle. Modeling and simulation can help manage risk by providing information on design capabilities and failure modes during the early stages of design. This allows initial design concepts to be iterated without having to build hardware for testing. The test and evaluation community can use predictive simulations to focus the use of valuable test assets on critical test issues. They can also use extrapolated simulations to expand the scope of evaluation into areas not readily testable, thus reducing the risk of having the system fail in the outer edges of the "test envelope." Additionally, a model can serve as a framework to bridge the missing pieces of a complete system until those pieces become available.

Although modeling and simulation can be a very effective risk-handling tool, it requires resources, commitment to refine models as the system under development matures, and a concerted verification and validation effort to ensure that decisions are based on credible information.

Key Parameter Control Boards. When a particular parameter (such as system weight) is crucial to achieving the overall program requirements, a control board for that parameter may be appropriate. This board has representatives from all affected technical functions and may be chaired by the PD/PM. It provides management focus on the parameter and signals the importance of achieving the parameter to the technical community. If staffed properly by all affected disciplines, it can also help avoid sacrificing other program requirements to achieve that requirement.

Manufacturing Screening. For programs in late and early production and deployment, various manufacturing screens (including environmental stress screening) can be incorporated into test article production and low-rate initial production to identify deficient manufacturing processes. Environmental stress screening is a manufacturing process for stimulating parts and workmanship defects in electronic assemblies and units. These data can then be used to develop the appropriate corrective actions.

Procedures. Risk control involves developing a risk-reduction plan, with actions identified, resourced, and scheduled. Success criteria for each of the risk-reduction events should also be identified. The effectiveness of these actions must be monitored using the types of techniques described in Section 6.6.

6.5.3 Risk Avoidance

Description. This technique reduces risk through the modification or elimination of those operational requirements, processes or activities that cause the risks. Eliminating operational requirements requires close coordination with the users. Since this technique results in the reduction of risk, it should generally be initiated in the development of a risk-handling plan. It can be done in parallel with the initial operational requirements analysis and should be supported by a cost-benefit analysis.

Procedures. Analyzing and reviewing the proposed system in detail with the user is essential to determine the drivers for each operational requirement. Operational requirements scrubbing involves eliminating those that have no strong basis. This also provides the PD/PM and the user with an understanding of what the real needs are and allows them to establish accurate system requirements for the critical performance. Operational requirements scrubbing essentially consists of developing answers to the following questions:

- Why is the requirement needed?
- What will the requirement provide?
- How will the capability be used?
- Are requirements specified in terms of functions and capabilities, rather than by specific design?

Cost/requirement trade studies are used to support operational requirements scrubbing. These trades examine each requirement and determine the cost to achieve various levels of the requirement (e.g., different airspeeds, range, payloads). The results are then used to determine, with the user, whether a particular requirement level is worth the cost of achieving that level. Trade studies are an inherent part of the systems engineering process.

6.5.4 Risk Assumption

Description. This technique is used in every project and acknowledges the fact that, in any project, risks exist that will have to be accepted without any special effort to control them. Such risks may be either inherent in the project or may result from other risk-controlling actions (residual risks). The fact that risks are assumed does not mean that they are ignored. In fact, every effort should be made to identify and understand them so that appropriate management action can be planned. Also, risks that are assumed should be monitored during development; this monitoring should be well planned from the beginning.

Procedures. In addition to the identification of risks to be assumed, the following steps are key to successful risk assumption:

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it materializes. This includes identifying the specific management actions that will be used, for example, redesign, retesting, requirements review, etc.
- Whenever a risk is assumed, a schedule and cost risk reserve should be set aside to cover the specific actions to be taken if the risk occurs. If this is not possible, the project may proceed within the funds and schedule allotted to the effort. If the project cannot achieve its objectives, a decision must be made to allocate additional resources, accept a lower level of capability (lower the requirements), or cancel the effort.
- Ensure that the necessary administrative actions are taken to quickly report on the risk event and implement these management actions, such as contracts for industry expert consultants, arrangements for test facilities, etc., and report on risk occurrences.

6.5.5 Risk Transfer

Description. This technique involves the reduction of risk exposure by the reallocation of risk from one part of the system to another or the reallocation of risks between the Government and the prime contractor, or between the prime contractor and its sub-contractor.

Procedures. In reallocating risk, design requirements that are risk drivers are transferred to other system elements, which may result in lower system risk but still meet system requirements. For example, a high risk caused by a system timing requirement may be lowered by transferring that requirement from a software module to a specially designed hardware module capable of meeting those needs. The effectiveness of requirements reallocation depends on good system engineering and design techniques. In fact, efficient allocation of those requirements that are risk drivers is an integral part of the systems engineering process. Modularity and functional partitioning are two design techniques that can be used to support this type of risk transfer. In some cases, this approach may be used to concentrate risk areas in one area of the system design. This allows management to focus attention and resources on that area.

For the Government/contractor risk-transfer approach to be effective, the risks transferred to the contractor must be those that the contractor has the capacity to control and manage. These are generally risks associated with technologies and processes used in the project—those for which the contractor can implement proactive solutions. The types of risks that are best managed by the Government include those related to the stability of and external influences on project requirements, funding, and schedule, for example. The contractor can support the management of these risks through the development of flexible project plans, and the incorporation of performance margins in the system and flexibility in the schedule. A number of options are available to implement risk transfer from the Government to the contractor: warranties, cost incentives, product performance incentives, and various types of fixed price contracts. A similar assessment of prime contractor versus sub-contractor allocation of risks can also be developed and used to guide risk transfer between these parties.

6.6 Risk Monitoring

6.6.1 General

Risk monitoring is a continuous process to systematically track and evaluate the performance of risk-handling actions against established metrics throughout the acquisition process. It should also include results of periodic reassessments of project risk to evaluate both known and new risks to the project. If necessary, the PD/PM should reexamine the risk-handling approaches for effectiveness while conducting assessments. As the project progresses, the monitoring process will identify the need for additional risk-handling options.

An effective monitoring effort provides information to show if handling actions are not working and which risks are on their way to becoming actual problems. The information should be available in sufficient time for the PD/PM to take corrective action. The functioning of IPTs is crucial to effective risk monitoring. They are the “front line” for obtaining indications that handling efforts are achieving their desired effects.

The establishment of a management indicator system that provides accurate, timely, and relevant risk information in a clear, easily understood manner is key to risk monitoring. Early in the planning phase of the process, PDs/PMs should identify specific indicators to be monitored and information to be collected, compiled, and reported. Usually, documentation and reporting procedures are developed as part of risk management planning before contract award and should use the contractor’s reporting system. Specific procedures and details for risk reporting should be included in the risk management plans prepared by the Government and the contractor.

To ensure that significant risks are effectively monitored, handling actions (which include specific events, schedules, and “success” criteria) developed during previous risk management phases should be reflected in integrated program planning and scheduling. Identifying these handling actions and events in the context of WBS elements establishes a linkage between them and specific work packages, making it easier to determine the impact of actions on cost, schedule, and performance. The detailed information on risk-handling actions and events should be contained in various risk management documentation (both formal and informal). Experience has shown that the use of an electronic on-line database that stores and permits retrieval of risk-related information is almost essential to effective risk monitoring. The database selected or developed will depend on the project. A discussion of Risk Management Information Systems and databases and suggested data elements to be included in the databases is contained later in this Section.

Many techniques and tools are available for monitoring the effectiveness of risk-handling actions, and project personnel should select those that best suit their needs. Some monitoring techniques include:

Test-Analyze-And-Fix (TAAF). Test-Analyze-And-Fix is the use of a period of dedicated testing to identify and correct deficiencies in a design. It was originally conceived as an approach to improve reliability; it can also be used for any system parameter whose development could benefit from a dedicated period of testing and analysis. Although it is a valuable aid in the development process, Test-Analyze-And-Fix should not be used in lieu of a sound design process.

Demonstration Events. Demonstration events are points in the project (usually tests) that are used to determine if risks are being successfully abated. Careful review of the planned development of each risk area will reveal a number of opportunities to verify the effectiveness of the development approach. By including a sequence of demonstration events throughout the development, PD/PM can monitor the process and identify when additional efforts are needed. Demonstration events can also be used as information-gathering actions, as discussed before, and as part of the risk-monitoring process. Table 10 contains examples of demonstration events.

Table 10. Examples of Demonstration Events

Item	Demonstration Event	Completion Date
Rocket Motor	Three Case Burst Tests Propellant Characterization Thermal Barrier Bond Tests Ignition and Safe/Arm Tests Nozzle Assembly Tests 10 Development Motor Firings -- Temperature and Altitude Cycle -- Vibration and Shock -- Aging	By completion of preliminary design By completion of final design
Central Computer	Test Breadboard Develop/Test Unique Microcircuits Build/Test Prototype	By completion of preliminary design By completion of final design

Process Proofing. When particular processes, especially those of manufacturing and support, are critical to achieving system requirements, an early process proof demonstration is useful to abate risk. If the initial proof is unsuccessful, time is still available to identify and correct deficiencies or to select an alternative approach.

No single technique or tool is capable of providing a complete answer—a combination must be used. In general, risk monitoring techniques are applied to follow through on the planned actions of the risk-handling program. They track and evaluate the effectiveness of handling activities by comparing planned actions with what is actually achieved. These comparisons may be as straightforward as actual versus planned completion dates, or as complex as detailed analysis of observed data versus planned profiles. In any case, the differences between planned and actual data are examined to determine status and the need for any changes in the risk-handling approach.

Project personnel should also ensure that the indicators/metrics selected to monitor project status adequately portray the true state of the risk events and handling actions. Otherwise, indicators of risks that are about to become problems will go undetected. Subsequent sections identify specific techniques and tools that will be useful to PDs/PMs in monitoring risks and provide information on selecting metrics that are essential to the monitoring effort. The techniques focus primarily at the program level, addressing cost, schedule, and performance risks.

6.6.2 Earned Value Management

Description. Earned value is a management technique that relates resource planning to schedules and to technical performance requirements. It is useful in monitoring the effectiveness of risk-handling actions in that it provides periodic comparisons of the actual work accomplished in terms of cost and schedule with the work planned and budgeted. These comparisons are made using a performance baseline that is established by the contractor and the PD at the beginning of the contract period. This is accomplished through an integrated baseline review process. The baseline must capture the entire technical scope of the project in detailed work packages. The baseline also includes the schedule to meet the requirements as well as the resources to be applied to each work package. Specific risk-handling actions should be included in these packages.

Procedures. The periodic earned value data can provide indications of risk and the effectiveness of handling actions. When variances in cost or schedule begin to appear in work packages containing risk-handling actions, or in any work package, the IPT can analyze the data to isolate causes of the variances and gain insights into the need to modify or create handling actions.

6.6.3 *Technical Performance Measurement*

Description. Technical performance measurement is a technique that compares estimated values of key performance parameters with achieved values, and determines the impact of any differences on system effectiveness. This technique can be useful in risk monitoring by comparing planned and achieved values of parameters in areas of known risk. The periodic application of this technique can provide early and continuing predictions of the effectiveness of risk-handling actions or the detection of new risks before irrevocable impacts on the cost or schedule occur.

Procedures. The technical performance parameters selected should be those that are indicators of progress in the risk-handling action employed. They can be related to system hardware, software, human factors, and logistics—any product or functional area of the system. Parameter values to be achieved through the planned handling action are forecast in the form of planned performance profiles. Achieved values for these parameters are compared with the expected values from the profile, and any differences are analyzed to get an indication of the effectiveness of the handling action. For example, suppose a system requires the use of a specific technology that is not yet mature and the use of which has been assessed as high risk. The handling technique selected is risk control, and an off-line technology maturation effort will be used to get the technology to the level where the risk is acceptable. The technology is analyzed to identify those parameters that are key drivers, and performance profiles that will result from a sufficiently mature technology are established. As the maturation effort progresses, the achieved values of these parameters are compared with the planned profile. If the achieved values meet the planned profile, it is an indicator that the risk-handling approach is progressing satisfactorily; if the achieved values fall short of the expected values, it is an indicator that the approach is failing to meet expectations and corrective action may be warranted.

6.6.4 *Integrated Planning and Scheduling*

Description. Once a contract has been awarded, techniques such as integrated planning and scheduling (integrated master plans and integrated master schedules) can become invaluable project baseline and risk-monitoring tools. Integrated planning identifies key events, milestones, reviews, all integrated technical tasks, and risk-reduction actions for the project, along with accomplishment criteria to provide a definitive measure that the required maturity or progress has been achieved. Integrated scheduling describes the detailed tasks that support the significant activities identified in integrated planning and timing of tasks. Also, the integrated schedule can include the resources planned to complete the tasks. The events, tasks, and schedule resulting from integrated planning are linked with contract specification requirements, WBS, and other techniques. When the events and tasks are related to risk-reduction actions, this linkage provides a significant monitoring tool, giving specific insights into the relationships among cost, schedule, and performance risks.

Procedures. In integrated planning, the Government and contractor (or other performing activity) should identify key activities of the project, to include risk-handling actions and success criteria. The contractor should then prepare the integrated schedule reflecting the planned completion of tasks associated with these activities. As the project progresses, the PD/PM can monitor effectiveness of handling activities included in the integrated planning events and schedule by comparing observed activity results with their criteria and determining any deviations from the planned schedule. Any failures of handling actions to meet either the event criteria or schedule should be analyzed to determine the deviation's impact, causes, and need for any modifications to the risk-handling approach.

6.6.5 Watch List

Description. The watch list is a listing of critical areas which management should pay special attention to during project execution. It is a straight-forward, easily prepared document that can range in complexity from a simple list of the identified risks to one that includes such things as the priority of the risk, how long it has been on the watch list, the handling actions, planned and actual completion dates for handling actions, and explanations of any differences. See Table 11 for an example watch list.

Table 11. Watch List Example

Potential Risk Area	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
• Accurately predicting shock environment shipboard equipment will experience.	• Use multiple finite element codes & simplified numerical models for early assessments. • Shock test simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SEA 03P31 SEA 03P31	31 Aug 01 31 Aug 02		
• Evaluating acoustic impact of the ship systems that are not similar to previous designs.	• Concentrate on acoustic modeling and scale testing of technologies not demonstrated successfully in large-scale tests or full-scale tests. • Factor acoustic signature mitigation from isolated modular decks into system requirements. Continue model tests to validate predictions for isolated decks.	SEA 03TC SEA 03TC	31 Aug 01 31 Aug 02		

Procedures. Watch list development is based on the results of the risk assessment. It is common to keep the number of risks on the watch list relatively small, focusing on those that can have the greatest impact on the project. Items can be added as the project unfolds and periodic reassessments are conducted. If a considerable number of new risks are significant enough to be added to the watch list, it may be an indicator that the original assessment was not accurate and that project risk is greater than initially thought. It may also indicate that the project is on the verge of becoming out of control. If a risk has been on the watch list for a long time because of a lack of risk-handling progress, a reassessment of the risk or the handling approach may be necessary. Items on the watch list should be reviewed during the various program reviews/meetings, both formal and informal.

6.7.6 Reports

Description. Reports are used to convey information to decision makers and project team members on the status of risks and the effectiveness of risk-handling actions. Risk-related reports can be presented in a variety of ways, ranging from informal verbal reports when time is of the essence to formal summary-type reports presented at milestone reviews. The level of detail presented will depend on the audience.

Procedures. Successful risk management programs include timely reporting of results of the monitoring process. Reporting requirements and procedures, to include format and frequency, are normally developed as part of risk management planning and are documented in the risk management plan. Reports are normally prepared and presented as part of routine program management activities. They can be effectively incorporated into program management reviews and technical milestones to indicate any technical, schedule, and cost barriers to the program objectives and milestones being met. One example of a status presentation is shown in Figure 22. It shows some top-level risk information that can be useful to the PD/PM as well as others external to the program.

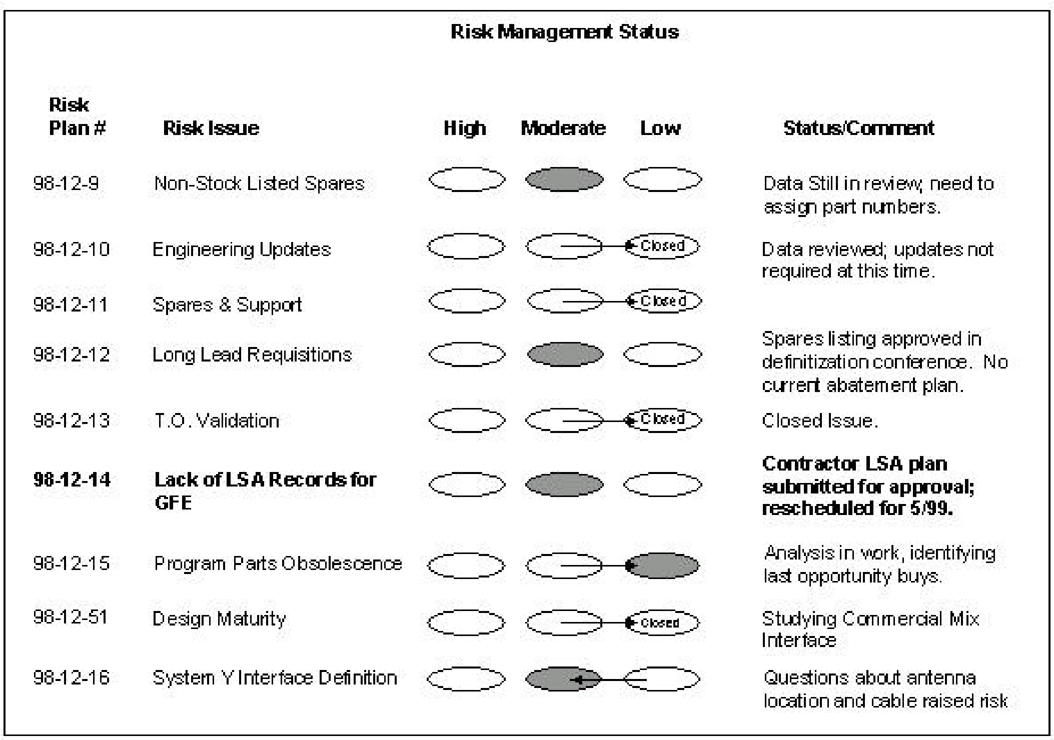


Figure 22. Example Showing Detailed List of Top-Level Risk Information

Although this level of reporting can provide quick review of overall risk status for identified problems, more detailed risk planning and status can be provided on individual risk items. For example, some project IPTs have combined risk level and scheduled activities to provide a graphical overview of risk status for either internal or external review. One method for graphically showing risk status for an individual item is shown in Figure 23.

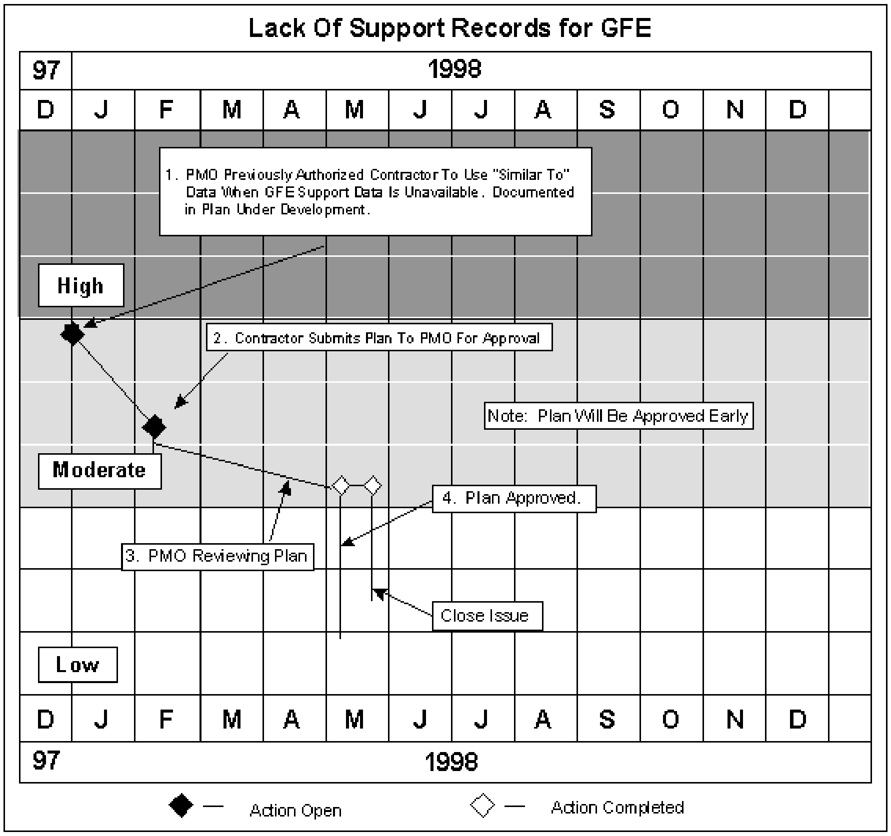


Figure 23. Example of More Complex Combination of Risk Level and Scheduled Tasks

6.6.7 Management Indicator System

Description. A management indicator system is a set of indicators or metrics that provide the PD/PM with timely information on the status of the project and risk-handling actions, and is essential to risk monitoring and project success. To be meaningful, these metrics should have some objective value against which observed data can be measured, reflecting trends in the project or lack thereof. Metrics should be developed jointly by the PD/PM. The contractor's approach to metrics should be a consideration in the proposal evaluation process. If the contractor does not have an established set of metrics, this may be an area of risk that will need to be addressed.

Procedures. Metrics can be categorized as relating to technical performance, cost, and schedule. Technical performance metrics can be further broken down into categories such as engineering, production, and support, and within these groups as either product-or process—related. Product-related metrics pertain to characteristics of the system being developed; they can include such things as planned and demonstrated values of the critical parameters monitored as part of the performance measurement process and system-unique data pertaining to the different steps in the development and acquisition processes. Table 12 provides examples of product-related metrics.

Table 12. Examples of Product-Related Metrics

Engineering	Requirements	Support	Production
• Key Design Parameters – Weight – Size – Endurance – Range • Design Maturity – Open problems reports – Number of engineering change proposals – Number of drawings released – Failure activities • Computer Resource Utilization	• Requirements Traceability • Requirements Stability	• Manufacturing Yields • Incoming Material Yields • Delinquent Requisitions • Unit Production Cost • Process Proofing	• Special Tools and Test Equipment • Support Infrastructure Footprint • Manpower Estimates

Process metrics pertain to the various processes used in the development and production of the system. For each project, certain processes are critical to the achievement of project objectives. Failure of these processes to achieve their requirements is symptomatic of significant problems. Metrics data can be used to diagnose and aid in problem resolution. They should be used in formal, periodic performance assessments of the various development processes and to evaluate how well the system development process is achieving its objectives. Table 14 provides examples of process-related metrics. Cost and schedule metrics can be used to depict how the project is progressing toward completion. The information provided by the contractor in the earned value management system can serve as these metrics, showing how the actual work accomplished compares with the work planned in terms of schedule and cost. Other sources of cost and schedule metrics include the contractor’s cost accounting information and the integrated master schedule. Table 14 provides examples of cost and schedule metrics.

Table 14. Examples of Process Metrics

Design Requirements	Trade Studies	Design Process	Integrated Test Plan	Failure Reporting System	Manufacturing Plan
• Development of requirements traceability plan • Development of specification tree • Specifications reviewed for: – Definition of all use environments – Definition of all functional requirements for each mission performed	• Users needs prioritized • Alternative system configurations selected • Test methods selected	• Design requirements stability • Producibility analysis conducted • Design analyzed for: – Cost – Parts reduction – Manufactur-ability – Testability	• All developmental tests at system and subsystem level identified • Identification of who will to test (Government, contractor, supplier)	• Contractor corporate-level management involved in failure reporting and corrective action process • Responsibility for analysis and corrective action assigned to specific individual with closeout date	• Plan documents methods by which design to be built • Plan contains sequence and schedule of events at contractor and subcontractor levels that defines use of materials, fabrication flow, test equipment, tools, facilities, and personnel • Reflects manufacturing inclusion in design process. Includes identification and assessment of design facilities

Table 15. Examples of Cost and Schedule Metrics

Cost	Schedule
Cost variance Cost performance index Estimate at completion Management reserve	Schedule variance Schedule performance index Design schedule performance Manufacturing schedule performance Test schedule performance

6.7 Risk Management Information Systems and Documentation

6.7.1 Description

To manage risk, PDs/PMs should have a database management system that stores and allows retrieval of risk-related data. The risk-management information system provides data for creating reports and serves as the repository for all current and historical information related to risk. This information may include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The PD/PM should consider a number of factors in establishing the management information system and developing rules and procedures for the reporting system:

- Assign management responsibility for the reporting system
- Publish any restrictions for entering data into the database

- Identify reports and establish a schedule, if appropriate
- Use standard report formats as much as possible
- Ensure that the standard report formats support all users, such as the PD, IPT, and contractors
- Establish policy concerning access to the reporting system and protect the database from unauthorized access.

With a well-structured information system, a PD/PM may create reports for senior management and retrieve data for day-today project management. Most likely, the PD/PM will choose a set of standard reports that suits specific needs on a periodic basis. This eases definition of the contents and structure of the database. In addition to standard reports, the PD/PM will need to create ad hoc reports in response to special queries, etc. Commercial database programs now available allow the PD/PM to create reports with relative ease. Figure 24 shows a concept for a management and reporting system.

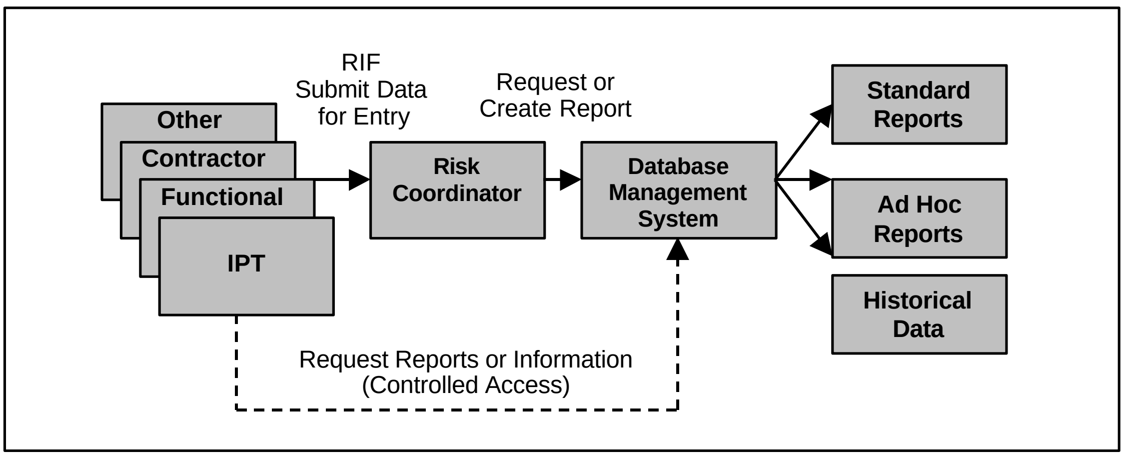


Figure 24. Conceptual Risk Management and Reporting System

6.7.2 *Risk Management Reports*

The following are examples of basic reports that a PD/PM may use to manage its risk program. Each office should tailor and amplify them, if necessary, to meet specific needs.

Risk Information Form. The PD/PM needs a document that serves the dual purpose of a source of data entry information and a report of basic information for the IPT. The Risk Information Form serves this purpose. It gives members of the project team, both Government and contractors, a format for reporting risk-related information. The Risk Information Form should be used when a potential risk event is identified and updated over time as information becomes available and the status changes. As a source of data entry, the Risk Information Form allows the database administrator to control entries. To construct the database and ensure the integrity of data, the PD/PM should design a standard format for a Risk Information Form.

Risk Assessment Report. Risk assessments form the basis for many project decisions, and the PD/PM will probably need a detailed report of any assessment of a risk event. A Risk assessment report is prepared by the team that assessed a risk event and amplifies the information in the Risk Information Form. It documents the identification and analysis process and results. This report provides information for the summary contained in the Risk Information Form, is the basis for developing risk-handling plans, and serves as a historical recording of program risk assessment. Since assessment reports may be large documents, they may be stored as files. Assessment reports should include information that links it to the appropriate Risk Information Form.

Risk-Handling Documentation. Risk-handling documentation may be used to provide the PD/PM with the information he needs to choose the preferred mitigation option and is the basis for the handling plan summary that is contained in the Risk Information Form. This document describes the examination process for the risk handling options and gives the basis for the selection of the recommended choice. After the PD/PM chooses an option, the rationale for that choice may be included. There should be a plan for each risk-mitigation task. Risk-handling plans are based on results of the risk assessment. This document should include information that links it to the appropriate Risk Information Form.

Risk Monitoring Documentation. The PD/PM needs a summary document that tracks the status of high and moderate risks. He can produce a risk-tracking list, for example, that uses information that has been entered from the Risk Information Form. Each PD/PM should tailor the tracking list to suit its needs. If elements of needed information are not included in the Risk Information Form, they should be added to that document to ensure entry into the database.

Database Management System. The database management system that the PD/PM chooses may be commercial, Government-owned, or contractor-developed.

It should provide the means to enter and access data, control access, and create reports. Many options are available to users.

Key to the management information system are the data elements that reside in the database. The items listed in Table 16 are examples of risk information that might be included in a database that supports risk management. They are a compilation of several risk reporting forms and other risk document sources. “Element” is the title of the database field; “Description” is a summary of the field contents. PDs/PMs should tailor the list to suit their needs.

Table 16. Database Management System Elements

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PD/PM. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PD/PM compared to all other risks, e.g., a one (1) indicates the highest priority.
Data Submitted	Gives the date that the Risk Information Form was submitted.
Major System/ Component	Identifies the major system/component based on the WBS.
Subsystem/ Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) or the risk.
Description of Risk	Briefly describes the risk. Lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, include how it is manifested (e.g., design & engineering, manufacturing, etc.)
Key Parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report, if appropriate.
Analyses	Briefly describes the analysis done to assess the risk. Includes rationale and basis for results.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's RMP.
Consequence	States the consequence of the event if it occurs, based on definitions in the program's RMP.
Time Sensitivity	Estimates the relative urgency for implementing the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measures using metrics for tracking progress in implementing risk-handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk handling milestones.
Status Due Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

6.8 Software Risk Management Methodologies

The management of risk in software intensive project is essentially the same as for any other type of project. A number of methodologies specifically focus on the software aspects of developmental project and can be useful in identifying and analyzing risks associated with software. Several of these methodologies are described in the U.S. Air Force publication, *Guide to Software Acquisition and Management.* Three of these methodologies are described below.

6.8.1 Software Risk Evaluation

This is a formal approach developed by the Software Engineering Institute using a risk management paradigm that defines a continuous set of activities to identify, communicate, and resolve software risks. These activities are to identify, analyze, plan, track, and control. (The Software Engineering Institute activities are analogous to the activities of the risk management process defined in this section.)

This methodology is initiated by the PD/PM, who tasks an independent software risk evaluation team to conduct a risk evaluation of the contractor's software development effort. The team executes the following software risk evaluation functions in performing this evaluation, and prepares findings that will provide the PD/PM with the results of the evaluation:

- Detection of the software technical risks present in the project. An software risk evaluation Taxonomy-Based Questionnaire is used to ensure that all areas of potential risk are identified. This questionnaire is based on the software risk evaluation Software Development Risk Taxonomy, which provides a systematic way of organizing and eliciting risks within a logical framework.
- Specification of all aspects of identified technical software risks, including their conditions, consequences/impacts, and source.
- Assessment of the risks to determine the probability of risk occurrence and the severity of its consequences/impacts.
- Consolidation of the risk data into a concise format suitable for decision making.

A detailed discussion of the SRE methodology is found in *Software Engineering Institute Technical Report* CMU/SEI-94-TR-19, *Software Risk Evaluation Model,* Version 1.0, December 1994.

6.8.2 Boehms Software Risk Management Method

This risk management methodology, developed by Barry W. Boehm and described in *IEEE Software, Software Risk Management: Principles and Practices,* January 1991, consists of two primary steps, each with three subordinate steps. This risk management structure is shown in Table 17.

Table 17. Software Risk Management Steps

Primary Steps	Secondary Steps	Description
Risk Assessment	Risk Identification	• Produces lists of project specific risk events
Risk Assessment	Risk Analysis	• Assesses probability of risk event and consequences • Assesses compound risk resulting from risk event interaction
Risk Assessment	Risk Prioritization	• Produces rank-ordered list of identified and analyzed risk events
Risk Control	Risk Management Planning	• Produces plan for addressing each risk event • Integrates individual risk event plans with each other and the overall plan
Risk Control	Risk Resolution	• Establishes the environment and actions to resolve or eliminate risks • Tracks progress in resolving risks
Risk Control	Risk Monitoring	• Provides feedback for refining prioritization and plans

Boehm provides a number of techniques that can be used to accomplish each of the steps in the methodology. For example, to assist in risk identification, he includes the top 10 top-level software risks, based on surveys of experienced software PDs/PMs. These risks are shown in Table 18, along with recommended techniques to manage them. Using this list as a starting point, managers and engineers can then develop lists of lower-level risks to be assessed and resolved.

Table 18. Top 10 Software Risks

Risk	Risk Management Techniques
Personnel Shortfalls	Staffing with top talent; job matching team building; key personnel agreements; cross training
Unrealistic schedules and budgets	Detailed multisource cost and schedule estimation; design-to-cost; incremental development; software reuse; requirements scrubbing
Developing the wrong software functions	Organizational analysis; mission analysis; operations concept formulation; user surveys; prototyping; early users' manuals
Developing wrong user interface	Task analysis; prototyping; scenarios; user characterization (functionality, style, workload)
Gold plating	Requirements scrubbing; prototyping; cost/benefit analysis; design-to-cost
Continuing stream of requirements changes	High change threshold; information hiding; incremental development (defer changes to later increments)
Shortfalls in externally furnished components	Benchmarking; inspections; reference checking; compatibility analysis
Shortfalls in internally performed tasks	Reference checking; pre-award audits; award-fee contracts; competitive design or prototyping; team building
Real-time performance shortfalls	Simulation; benchmarking; modeling; prototyping; instrumentation; tuning
Straining computer science capabilities	Technical analysis; cost-benefit analysis; prototyping; reference checking

6.8.3 Best Practices Initiative Risk Management Method

The Software Acquisition Best Practices Initiative was instituted in 1994 to improve and restructure the software acquisition management process through the identification of effective practices used in successful software developments. One result of this effort was the publication of the *Program Manager's Guide to Software Acquisition Best Practices* by the Software Program Managers Network. This document identified nine principal best practices that are essential to the success of any large-scale software development. The first of these nine is formal risk management. To assist in implementing this top practice, Software Program Managers Network developed a three-part methodology consisting of the following steps: address the problem; practice essentials; and check status. Specific activities associated with these steps are shown in Table 19.

Table 19. Best Practices Initiative Risk Management Method

Best Practices Initiative Risk Management Method		
Address the Problem	***Practice Essentials***	***Check Status***
• Recognize that all software has risk • Attempt to resolve risk as early as possible when cost impact is less than it will be later in development	• Identify risks • Decriminalize risk • Plan for risk • Formally designate a Risk Officer • Include in budget and schedule a risk reserve buffer of time, money, and other resources • Compile database for all non-negligible risks • Prepare profile for each risk showing probability and consequences • Include all risks over full life cycle • Provide frequent risk status reports that include: – Top 10 risk items – Number of risk items resolved – Number of new risk items – Number of risk items unresolved – Unresolved risk items on critical path • Probably costs for unresolved risks	• Risk Officer appointed? • Risk databases set up? • Risk assessments have clear impact on program plans and decisions? • Frequency and timeliness of risk assessment updates consistent with decision updates? • Objective criteria used to identify, assess, and manage risk? • Information flow patterns and reward criteria support identification of risk by all program personnel? • Risks identified throughout entire life cycle? • Risk management reserve exist? • Risk profile for every risk, and components updated regularly? • Risk management plan has explicit provisions for altering decision makers when risk becomes imminent?

The Software Program Managers Network provides PDs/PMs with specialized training programs covering the core disciplines and techniques for implementing this formal risk management practice, as well as the other best practices. This network also has available (or under development) a number of guidebooks designed to provide software developers and PDs/PMs with practical guidance for planning, implementing, and monitoring their projects.

Software Program Managers Network can be contacted at (703) 521-5231, or on the Internet at http://spmn.com/.

In addition to the studies by Barry Boehm, and information on the Software Program Managers Network, a survey was conducted by Conrow and Shishido which evaluated 10 prior studies and categorized the resulting risk issues across the studies into six categories and 17 total issues, as shown in Table 20. The very high degree of overlap between risk issues identified in the 10 underlying studies suggests that some risk issues are common to many software-intensive projects.

Table 20. Software Risk Grouping

Risk Grouping	Software Risk Issue
Project-Level	1. Excessive, immature, unrealistic or unstable requirements 2. Lack of involvement 3. Underestimation of project complexity or dynamic natures
Project Attributes	4. Performance shortfalls (includes errors and quality) 5. Unrealistic cost or schedule (estimates and/or allocated amounts)
Management	6. Ineffective project management (possible at multiple levels)
Engineering	7. Ineffective integration, assembly and test; quality control; specialty engineering; systems engineering or (possible at multiple levels) 8. Unanticipated difficulties associated with the user interface
Work Environment	9. Immature or untried design, processes or technologies selected 10. Inadequate work plans or configuration control 11. Inappropriate methods or tool selection or inaccurate metrics
Other	12. Poor planning 13. Inadequate or excessive documentation or review process 14. Legal or contractual issues (e.g., litigation, malpractice, ownership) 15. Obsolescence (includes excessive schedule length) 16. Unanticipated difficulties with subcontracted items 17. Unanticipated maintenance and/or support costs

APPENDIX 1

A-1. SAMPLE RISK MANAGEMENT PLAN

As stated in DOE Manual 413.3-1, “The project manager should develop a Risk Management Plan.” The purpose/objective of a Risk Management Plan (RMP) is to assist the PD/PM to properly focus on and adequately implement the six steps of a sound risk management strategy: (1) risk awareness; (2) risk identification; (3) risk quantification; (4) risk handling; (5) risk impact determination; and (6) risk reporting, tracking, and closeout.

To further assist the PD/PM in the risk management effort, and to lend structure and uniformity to the DOE risk management process, the following sample RMP is provided. Use of the sample is not mandatory. However, its use is recommended to help assure consistency among plans, and consideration of important, common areas when managing risk. When used, the sample Plan should be tailored to meet the needs of the project, not simply adopted as written.

The RMP sample format is a compilation of several risk plans, and represents the types of information and considerations that a plan, tailored to a specific project, might contain.

Introduction. This section should address the purpose and objective of the Plan, and provide a brief summary of the project, to include the approach being used to manage the project, and the acquisition strategy.

Project Summary. This section contains a brief description of the project, including the acquisition strategy and the project management approach. The acquisition strategy should address its linkage to the risk management strategy.

Definitions. Definitions used by the project should be consistent with DOE definitions for ease of understanding and consistency. However, the DOE definitions allow project managers flexibility in constructing their risk management programs. Therefore, each project’s RMP may include definitions that expand the DOE definitions to fit its particular needs. For example, each Plan should include, among other things, definitions for the ratings used for technical, schedule and cost risk.

Risk Management Strategy and Approach. Provide an overview of the risk management approach, to include the status of the risk management effort to date, and a description of the project risk management strategy.

Organization. Describe the project’s risk management organization and list the responsibilities of each of the risk management participants.

Risk Management Process and Procedures. Describe the project risk management process to be employed; i.e., risk planning, assessment, handling, monitoring and documentation, and a basic explanation of these components. Also provide application guidance for each of the risk management functions in the process. If possible, the guidance should be as general as possible to allow the project's risk management organization (e.g., integrated project team [IPT]) flexibility in managing risk, yet specific enough to ensure a common and coordinated approach to risk management. It should address how the information associated with each element of the risk management process will be documented and made available to all participants in the process, and how risks will be tracked, to include the identification of specific metrics if possible.

Risk Planning. This section describes the risk planning process and provides guidance on how it will be accomplished, and the relationship between continuous risk planning and this RMP. Guidance on updates of the RMP and the approval process to be followed should also be included

Risk Assessment. This section of the Plan describes the assessment process and procedures for examining the critical risk areas and processes to identify and document the associated risks. It also summarizes the analysis process for each of the risk areas leading to the determination of a risk rating. This rating is a reflection of the potential impact of the risk in terms of its variance from known best practices or probability of occurrence, its consequence/impact, and its relationship to other risk areas or processes. This section may include:

- Overview and scope of the assessment process
- Sources of information
- Information to be reported and formats
- Description of how risk information is documented
- Assessment techniques and tools.

Risk Handling. This section describes the procedures that can be used to determine and evaluate various risk handling options, and identifies tools that can assist in implementing the risk handling process. It also provides guidance on the use of the various handling options for specific risks.

Risk Monitoring. This section describes the process and procedures that will be followed to monitor the status of the various risk events identified. It should provide criteria for the selection of risks to be reported on, and the frequency of reporting. Guidance on the selection of metrics should also be included.

Risk Management Information System, Documentation and Reports. This section describes the Risk Management Information System structure, rules, and procedures that will be used to document the results of the risk management process. It also identifies the risk management documentation and reports that will be prepared; specifies the format and frequency of the reports; and assigns responsibility for their preparation.

A-2. Sample Risk Management Plan For The XYZ Project

1.0 Introduction

1.1 Purpose

This Risk Management Plan (RMP) presents the process for implementing proactive risk management as part of the overall management of the XYZ project. Risk management is a program management tool to assess and mitigate events that might adversely impact the project. Therefore, risk management increases the probability/likelihood of project success. This RMP will:

- Serve as a basis for identifying alternatives to achieve cost, schedule, and performance goals
- Assist in making decisions on budget and funding priorities
- Provide risk information for milestone decisions
- Allow monitoring the health of the project as it proceeds.

The RMP describes methods for identifying, analyzing, prioritizing, and tracking risk drivers; developing risk-handling plans; and planning for adequate resources to handle risk. It assigns specific responsibilities for the management of risk and prescribes the documenting, monitoring, and reporting processes to be followed.

1.2 Project Summary

The XYZ project was initiated in response to Mission Need Statement (MNS) XXX, dated DD-MM-YYYY and Functional and Operational Requirements Document, dated DD-MMYYYY. The project is required to support the fundamental objective of the DOE's mission and Strategic Plan. The XYZ project is based on the need for a radioactive waste treatment facility. The XYZ mission areas are: (Delineate applicable areas).

The XYZ project will develop and procure a waste processing facility to replace the aging ABC facility. In order to meet DOE objectives, the XYZ system must begin hot operation by FY-07. The project is commencing a two-year development phase that will be followed by a four-year design/procurement/construction phase. The objectives of the design phase are to (discuss the specific objectives of this phase). The project has Congressional interest.

1.2.1 System Description

Provide a brief description of the major systems/structures/facilities that comprise the project. Include capabilities throughput, unique design features, specialty items, etc.

1.2.2 Acquisition Strategy

The XYZ project initial strategy is to contract with the site M&I contractor for providing all phases of the XYX system. The M&I will be responsible to use the most appropriate subcontracting strategy to obtain needed support services.

1.2.3 Project Management Approach

The XYZ project is managed following the project management concepts defined in DOE Order 413.3, and integrated project team (IPT) established largely along the hierarchy of the product work breakdown structure (WBS). The PD chairs the IPT.

1.3 Definitions

1.3.1 Risk

Risk is a measure of the inability to achieve overall project objectives within defined cost, schedule, technical/scope constraints and has two components: (1) the *probability* of failing to achieve a particular outcome, and (2) the *consequences/impacts* of failing to achieve that outcome. For processes, risk is a measure of the difference between actual performance of a process and the known best practice for performing that process.

1.3.2 Risk Event

Risk events are those events within the XYZ project that, if they go wrong, could result in problems in the development, construction, and/or operation of the facility. Risk events should be defined to a level such that the risk and causes are understandable and can be accurately assessed in terms of probability/likelihood and consequence/impact to establish the level of risk. For processes, risk events are assessed in terms of process variance from known best practices and potential consequences/impacts of the variance.

1.3.3 Technical Risk

This is the risk associated with the evolution of the design and operation of the XYZ project deliverables affecting the level of performance necessary to meet the operational requirements. The contractor's and subcontractors' design, test, and production processes (process risk) influence the technical risk and the nature of the product as depicted in the various levels of the WBS (product risk).

1.3.4 Cost Risk

This is the risk associated with the ability of the project to achieve its life cycle cost objectives. Two risk areas bearing on cost are: (1) the cost estimates and objectives are accurate and reasonable, and (2) project execution will not meet the cost objectives as a result of a failure to handle cost, schedule, and performance risks.

1.3.5 Schedule Risk

Schedule risks are those associated with the adequacy of the time estimated and allocated for the development, design, construction, and operation of the facility/system. Two risk areas bearing on schedule risk are: (1) the schedule estimates and objectives are realistic and reasonable, and (2) project execution will fall short of the schedule objectives as a result of failure to handle cost, schedule, or performance risks.

1.3.6 Risk Ratings

Risk rating is the value given to a risk event (or the project overall) based on an analysis of the probability/likelihood and consequences/impacts of an event. For the XYZ project, risk ratings of Low, Moderate, or High will be assigned based on the following criteria. Section 3.3.2 of this appendix provides guidance on determining probability/likelihood and consequences/impacts. When rating process variance from best practices, there is no rating of probability/likelihood. The level would be a measure of the variance from best practices (Section 3.3.2.3).

- Low Risk: Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Actions within the scope of the planned project and normal management attention should result in controlling acceptable risk.
- Moderate Risk: May cause an increase in cost, disruption of schedule, or degradation of performance. Special action and management attention may be required to handle risk.
- High Risk: Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Significant additional action and high priority management attention will be required to handle risk.

1.3.7 Independent Risk Assessor

An independent risk assessor is a person who is not in the management chain or directly involved in performing the tasks being assessed. Use of independent risk assessors is a valid technique to ensure that all risk areas are identified and that the consequence/impact and probability/likelihood (or process variance) are properly understood. The technique can be used at different project levels, e.g., PD, contractors, suppliers, vendors, etc. The PD will approve the use of independent assessors, as needed.

1.3.8 Templates and Best Practices

A “template” is a disciplined approach for the application of critical engineering and manufacturing processes that are essential to the success of most projects.

1.3.9 Metrics

There are measures used to indicate progress or achievement.

1.3.10 Critical Program Attributes

Critical program attributes are performance, cost, and schedule properties or values that are vital to the success of the project. They are derived from various sources, such as the Acquisition Strategy, exit criteria for the next program phase, Key Performance Parameters, test plans, the judgment of project experts, etc. The XYZ project will track these attributes to determine the progress in achieving the final required value. See Attachment 1 for a list of the XYZ critical project attributes.

2.0 Risk Management Approach

2.1 General Approach and Status

DOE M 413.3-X, Chapter 9, indicates risks must be well understood, and risk management approaches developed, before decision authorities can authorize a program to proceed into the next phase of the acquisition process. Figure A-1 shows how the XYZ project risk management fits into the phases and milestones of the acquisition process.

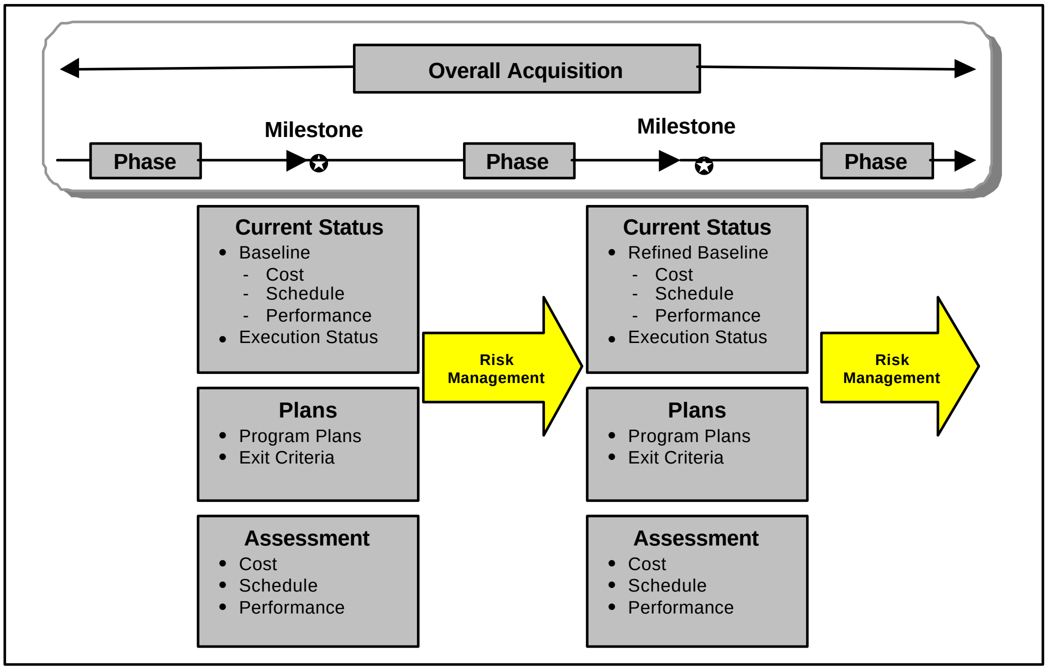


Figure A-1. Risk Management and the Acquisition Process

The XYZ project will use a centrally developed risk management strategy throughout the acquisition process and decentralized risk planning, assessment, handling, and monitoring. XYZ risk management is applicable to all acquisition functional areas.

The Initiation phase of the project identified potential risk events and the Acquisition Strategy reflects the project's risk-handling approach. Overall, the risk of the XYZ project was assessed as moderate, but acceptable. Moderate risk functional areas were technology, manufacturing, cost, funding, and schedule. The remaining functional areas of design and engineering (hardware and software), support, (schedule) concurrency, human systems integration, and environmental impact were assessed as low risk.

2.2 Risk Management Strategy

The basic risk management strategy is intended to identify critical areas and risk events, both technical and non-technical, and take necessary action to handle them before they become problems, causing serious cost, schedule, or performance impacts. This project will make extensive use of modeling and simulation, technology demonstrations, and prototype testing in handling risk.

Risk management will be accomplished using the IPT. The IPT should use a structured assessment approach to identify and analyze those processes and products that are critical to meeting project objectives. They then develop risk-handling options to mitigate the risks and monitor the effectiveness of the selected handling options. Key to the success of the risk management effort is the identification of the resources required to implement the developed risk-handling options. Important inputs to risk management include the identification of critical project attributes (Table A-1).

Table A-1. Critical Project Attributes

Category	Description	Responsible Entity	Remarks
Performance/Physical	Speed		
	Weight		
	Endurance		
	Crew Size		
	Operability		
	Availability		
	Size		
	Throughput		
	Recovery Time		
	Initial Setup		
	Identification Time		
	Reliability		
	Maintainability		
	Availability		
Cost	Operating and Support Costs		
	Construction Costs		
Processes	Requirements Stable		
Testing	**Systems and Equipment**		
	Laboratory Plans		
	Pilot Plans		
	Accuracy Verified by Test Data and Analysis		

Risk information is captured by the IPT in a Risk Management Information System using a standard Risk Information Form. The Risk Management Information System provides reports and is capable of preparing *ad hoc* tailored reports.

Risk information will be included in all project reviews, and as new information becomes available, the PD/PM will conduct additional reviews to ascertain if new risks exist. The goal is to be continuously looking to the future for areas that may severely impact the program.

2.3 Organization

The risk organization for the XYZ program is shown in Figure A-2. This is *not* a separate organization, but rather shows how risk is integrated into the project's existing organization and shows risk relationships among members of the project team.

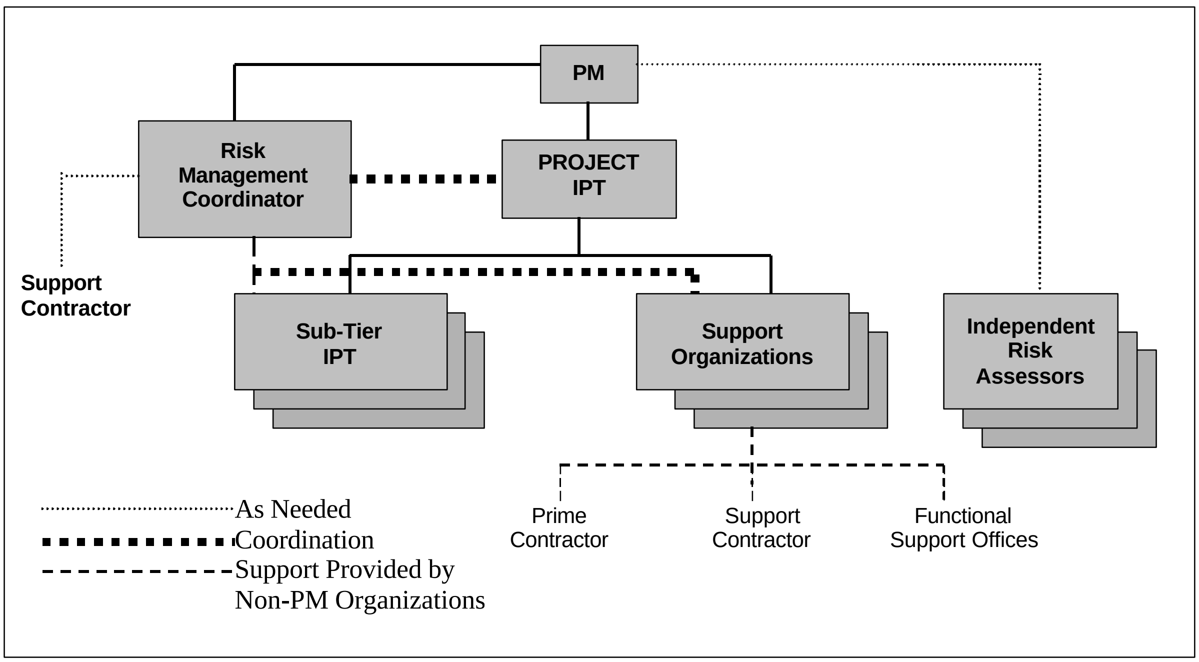


Figure A-2. XYZ Risk Management Organization

2.3.1 Risk Management Coordinator

The Risk Management Coordinator is the overall coordinator of the project's Risk Management Program. The Risk Management Coordinator is responsible for:

- Maintaining this RMP
- Maintaining the Risk Management Database

- Briefing the PD/PM on the status of XYZ project risk
- Tracking efforts to reduce moderate and high risk to acceptable levels
- Providing risk management training
- Facilitating risk assessments
- Preparing risk briefings, reports, and documents required for oroject reviews and the acquisition milestone decision processes.

2.3.2 Integrated Project Team

The IPT is responsible for complying with the DOE risk management policy and for structuring an efficient and useful XYZ risk management approach. The PD/PM is the Chair of the IPT. The IPT membership may be adjusted as the project progresses.

The IPT is responsible for implementing risk management tasks per this Plan. This includes the following responsibilities:

- Review and recommend to the Risk Management Coordinator changes on the overall risk management approach based on lessons learned
- Quarterly, or as directed, update the project risk assessments made during the project Initiation phase
- Review and be prepared to justify the risk assessments made and the risk mitigation plans proposed
- Report risk to the PD/PM, with information to the Risk Management Coordinator via Risk Information Forms
- Ensure that risk is a consideration at each program review.

2.3.3 XYZ Independent Risk Assessors

Independent Assessors made a significant contribution to the XYZ risk assessments. The use of independent assessments is a means of ensuring that all risk areas are identified. The use of independent risk assessors will continue on an as needed basis.

2.3.4 User Participation

The user/owner organization is responsible for remaining fully involved in the risk management process, and identifying risks associated with system/facility operation (e.g., trained personnel).

2.3.5 Risk Training

The key to the success of the risk efforts is the degree to which all members of the team, both the DOE and contractor are properly trained. The XYZ project will provide risk training, or assign members to training classes, during project Initiation. Key personnel with

XYZ management or assessment responsibilities are required to attend. All members of the team receive, at a minimum, basic risk management training. XYZ sponsored training is planned to be presented according to the schedule provided in Attachment X (not provided).

3.0 Risk Management Process and Procedures

3.1 Overview

This section describes the XYZ project risk management process and provides an overview of the XYZ risk management approach. The DOE defines risk management as the act or practice of controlling risk. It includes risk planning, assessing risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program. Figure A-3 shows, in general terms, the overall risk management process that will be followed in the XYZ project. This process follows DOE policies and guidelines and incorporates ideas found in other sources. Each of the risk management functions shown in Figure A-3 is discussed in the following paragraphs, along with specific procedures for executing them.

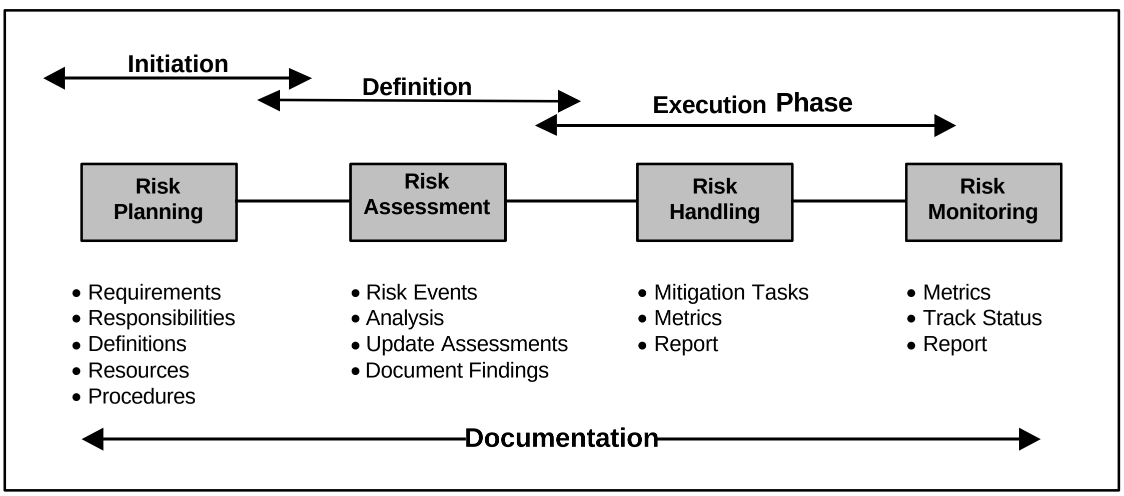


Figure A-3. Risk Management Structure (also referred to as the Risk Management Process Model)

3.2 Risk Planning

3.2.1 Process

Risk planning consists of the up-front activities necessary to execute a successful risk management program. It is an integral part of normal project planning and management. The planning should address each of the other risk management functions, resulting in an organized and thorough approach to assess, handle, and monitor risks. It should also assign responsibilities for specific risk management actions and establish risk reporting and documentation requirements. This RMP serves as the basis for all detailed risk planning, which must be continuous.

3.2.2 Procedures

3.2.2.1 Responsibilities. Each IPT is responsible for conducting risk planning, using this RMP as the basis. Planning covers all aspects of risk management to including assessment, handling options, and monitoring of risk mitigation activities. The Project Risk Management Coordinator monitors the planning activities of the IPT to ensure that they are consistent with this RMP and that appropriate revisions to this plan are made when required to reflect significant changes resulting from the IPT planning efforts.

Each person involved in the design, production, operation, support, and eventual disposal of the XYZ system or any of its systems or components is a part of the risk management process. This involvement is continuous and should be considered a part of the normal management process.

3.2.2.2 Resources and Training. An effective risk management program requires resources. As part of its planning process, each IPT will identify the resources required to implement the risk management actions. These resources include time, material, personnel, and cost. Training is a major consideration. All IPT members should receive instruction on the fundamentals of risk management and special training in their area of responsibility, if necessary.

3.2.2.3 Documentation and Reporting. This RMP establishes the basic documentation and reporting requirements for the project. IPTs should identify any additional requirements that might be needed to effectively manage risk at their level. Any such additional requirements must not conflict with the basic requirements in this RMP.

3.2.2.4 Metrics. Each IPT should establish metrics to measure the effectiveness of their planned risk-handling options. See Table A-2 for examples of metrics that may be used.

Table A-2. Examples of Product-Related Metrics

Engineering	Requirements	Support	Production
Key Design Parameters • Weight • Size • Throughput • Availability Design Maturity • Open problems reports • Number of change proposals • Number of drawings released • Failure activities • Computer Resource Utilization	Requirements Traceability Requirements Stability Design Mission Profile	Manufacturing Yields Incoming Material Yields Unit Production Cost Process Proofing Waste Personnel Stability	Special Tools and Test Equipment Support Infrastructure Footprint Manpower Estimates

Table A-2. Examples of Process Metrics

Design Requirements	Trade Studies	Design Process	Integrated Test Plan	Failure Reporting System	Construction Plan
Development of requirements document Development of specifications and drawings Definiiton of NEPA Strategy Development of Safety Documentation Identification of project interfaces	Users needs prioritized Alternative system configuratio ns selected Test methods selected	Design requirements stability Producibility analysis conducted Design analyzed for: • Cost • Schedule • Constructability • Operability • Testability	All developmental tests at system and subsystem level identified Identification of who performs test (DOE, contractor, supplier)	Contractor corporate-level management involved in failure reporting and corrective action process Responsibility for analysis and corrective action assigned to specific individual with closeout date	Plan documents methods by which design to be built Plan contains sequence and schedule of events at contractor and subcontractor levels that defines use of materials, fabrication flow, test equipment, tools, facilities, and personnel Reflects construction inclusion in design process. Includes identification and assessment of design facilities

Table A-2. Examples of Cost and Schedule Metrics

Cost	Schedule
Cost variance	Schedule variance
Cost performance index	Schedule performance index
Estimate at completion	Design schedule performance
Management reserve	Construction schedule performance
Estimate to Complete	Test schedule performance

3.2.2.5 Risk Planning Tools. The following tools can be useful in risk planning. It may be useful to provide this information to the contractors/subcontractors to help them understand the XYZ project's approach to managing risk. This list is not meant to be all-inclusive.

- DoD Manual 4245.7-M, a DoD guide for assessing process technical risk.
- The Navy's Best Practices Manual, NAVSO P-6071, provides additional insight into each of the Templates in DoD 4245.7-M and a checklist for each template.
- Program Manager's Work Station software, may be useful to some risk assessors. Program Manager's Work Station has a Risk Assessment module based on the Template Manual and Best Practices Manual.
- Commercial and Government developed risk management software.

The latter includes Government software, such as *Risk Matrix* developed by Mitre Corporation for the Air Force and the New Attack Submarine's *On-Line Risk Data Base*.

3.2.2.6 Plan Update. This RMP will be updated, if necessary, on the following occasions: (1) whenever the acquisition strategy changes, or there is a major change in project emphasis; (2) in preparation for major decision points (e.g., a Critical Decision submission); (3) in preparation for and immediately following technical audits and reviews; and (4) concurrent with the review and update of other project plans.

3.3 Risk Assessment

The risk assessment process includes the identification of critical risk events/processes, which could have an adverse impact on the project, and the analyses of these events/processes to determine the probability/likelihood of occurrence/process variance and consequences/impacts. It is the most demanding and time-consuming activity in the risk management process.

3.3.1 Process

3.3.1.1 Identification. Risk identification is the first step in the assessment process. The basic process involves searching through the entire XYZ project to determine those critical events that would prevent the project from achieving its objectives. All identified risks will be documented in the Risk Management Information System, with a statement of the risk and a description of the conditions or situations causing concern and the context of the risk.

Risks may be identified by the IPT, by any individual in the project, and by contractors/ subcontractors. The IPT and contract organizations can identify significant concerns earlier than otherwise might be the case and identify those events in critical areas that need to be dealt with to avoid adverse consequences/impacts. Likewise, individuals involved in the detailed and day-to-day technical, cost, and scheduling aspects of the project are most aware of the potential problems (risks) that need to be managed.

3.3.1.2 Analysis. This process involves:

- Identification of WBS elements
- Evaluation of the WBS elements using the risk areas to determine risk events
- Assignment of probability/likelihood and consequence/impact to each risk event to establish a risk rating
- Prioritization of each risk event relative to other risks.

Risk analysis should be supported by a study, test results, modeling and simulation, trade study, the opinion of a qualified expert (to include justification of his or her judgment), or any other accepted analysis technique. Evaluators should identify all assumptions made in assessing risk. When appropriate, a sensitivity analysis should be done on assumptions.

Systems engineering analysis, risk assessments, and manpower risk assessments provide additional information for consideration. This includes, among other things, environmental impact, system safety and health analysis, and security considerations. Projects may experience difficulties in access, facilities, and visitor control that can introduce risk and this must be considered.

The analysis of individual risk is the responsibility of the IPT, or the entity to which the risk has been assigned. They may use external resources for assistance, such as field activities, laboratories, and contractors. The results of the analysis of all identified risks must be documented in the Risk Management Information System.

3.3.2 Procedures

3.3.2.1 Assessments General. Risk assessment is an iterative process, with each assessment building on the results of previous assessments

For the project office, unless otherwise directed in individual tasking, project level risk assessments are presented at each project review meeting with a final update not later than 6 months before the next scheduled critical decision. The primary source of information for the next assessment is the current assessment baseline and existing documentation, the contract WBS, industry best practices, the Conceptual Design Report (CDR), the Performance Baseline (PB), and any contractor design documents.

The IPT should continually assess the risks, reviewing risk-mitigation actions and the critical risk areas whenever necessary to assess progress. For contractors, risk assessment updates should be made as necessary.

The risk assessment process is intended to be flexible enough so that field activities, laboratories, and contractors may use their judgment in structuring procedures considered most successful in identifying and analyzing all risk areas.

3.3.2.2 Identification. Following is a description of step-by-step procedures that evaluators may use as a guide to identify program risks.

Step One. Understand the requirements and the project performance goals, which are defined as thresholds and objectives. Describe the operational (functional and environmental) conditions under which the values must be achieved by referring or relating to design documents. The PB contains KPs.

Step Two. Determine the engineering and manufacturing processes that are needed to design, develop, produce, and support the project. Obtain industry best practices for these processes.

Step Three. Identify contract WBS elements (to include products and processes).

Step Four. Evaluate each WBS element against sources/areas of risk.

Step Five. Assign a probability and consequence/impact to each risk event

Step Six. Prioritize the risk events. Following are indicators the IPT may find helpful in identifying and assessing risk:

- Lack of Stability, Clarity, or Understanding of Requirements: Requirements drive the design of the system. Changing or poorly stated requirements guarantees the introduction of performance, cost, and schedule problems.
- Failure to Use Best Practices virtually assures that the project will experience some risk. The further a contractor deviates from best practices, the higher the risk.
- New Processes should always be suspect, whether they are related to design, analysis, or production. Until they are validated, and until the people who implement them have been trained and have experience in successfully using the process, there is risk.
- Any Process Lacking Rigor should also be suspect; it is inherently risky. To have rigor, a process should be mature and documented, it should have been validated, and it should be strictly followed.
- Insufficient Resources: People, funds, schedule, and tools are necessary ingredients for successfully implementing a process. If any are inadequate, to include the qualifications of the people, there is risk.
- Test Failure may indicate corrective action is necessary. Some corrective actions may not fit available resources, or the schedule, and (for other reasons as well) may contain risk.
- Qualified Supplier Availability: A supplier not experienced with the processes for designing and producing a specific product is not a qualified supplier and is a source of risk.
- Negative Trends or Forecasts are cause for concern (risk) and may require specific actions to turn around. There are a number of techniques and tools available for identifying risks, including:

  — Best Judgment: The knowledge and experience of the collective, multi-disciplined IPT members and the opinion of subject-matter experts are the most common source of risk identification.

  — Lessons Learned from similar processes can serve as a baseline for the successful way to achieve requirements. If there is a departure from the successful way, there may be risk.

  — DoD 4245.7-M, “Transition from Development to Production,” is often called the “Templates” book because it identifies technical risk areas and provides, in “bullet” form, suggestions for avoiding those risks. It focuses on the technical details of product design, test, and production to help managers proactively manage risk. It also includes chapters on facilities, logistics, and management, which make a useful tool in identifying weak areas of XYZ planned processes early enough to implement actions needed to avoid adverse consequences/impacts. A copy of this manual is available at: http://web7.whs.osd.mil/dodiss/publications/pub2.htm.

— The NAVSO P-6071 Best Practices Manual was developed by the Navy to add depth to the Template Book, DoD 4245.7-M.

— Critical Program Attributes are metrics that the project office develops to measure progress toward meeting objectives. Team members, IPTs, functional managers, contractors, etc., may develop their own metrics to support these measurements. The attributes may be specification requirements, contract requirements, or measurable parameters from any agreement or tasking. The idea is to provide a means to measure whether the project is on track in achieving our objectives.

— Methods and Metrics for Product Success is a manual published by the Office of the Assistant Secretary of the Navy Product Integrity Directorate. It highlights areas related to design, test, and production processes where problems are most often found and metrics for the measurement of effectiveness of the processes.

— Risk Matrix is another candidate for use by the PD/PM. It is an automated tool, developed by Mitre Corporation, that supports a structured approach for identifying risk and assessing its potential project impact. It is especially helpful for prioritizing risks.

— Requirements documents describe the output of risk efforts. IPT efforts need to be monitored continuously to ensure requirements are met on time and within budget. When they aren't, there is risk.

— Contracting for risk management helps ensure the people involved with the details of the technical processes of design, test, and production are involved with managing risk. The principle here is that those performing the technical details are normally the first ones to know risks exist.

— Quality Standards, such as ISO9000, ANSI/ASQC Q 9000, MIL-HDBK 9000, and others describe processes for developing and producing quality products. Comparing project processes with these standards can highlight areas for change to avoid risk.

— Use of Independent Risk Assessors is a method to help ensure all risk is identified. The knowledgeable, experienced people are independent from the management and execution of the processes and procedures being reviewed. Independent assessment promotes questions and observations not otherwise achievable.

3.3.2.3 Assessment. Risk assessment is an evaluation of the identified risk events to determine possible outcomes, critical process variance from known best practices, the probability/likelihood of those events occurring, and the consequences/impacts of the outcomes. Once this information has been determined, the risk event may be rated against the project's criteria and an overall assessment of low, moderate, or high assigned. Figure A-4 depicts the risk assessment process and procedures.

Critical Process Variance. For each process risk related event identified, the variance of the process from known standards or best practices must be determined. As shown in Figure A-4, there are five levels (a-e) in the XYZ risk assessment process, with the corresponding criteria of *Minimal, Small, Acceptable, Large, and Significant.* If there is no variance then there is no risk.

Level	What is the Likelihood the Risk Event Will Happen?
a	Remote
b	Unlikely
c	Likely
d	Highly Likely
e	Near Certainty

Process Variance refers to deviation from best practices.
Likelihood/Probability refers to risk events.

ASSESSMENT GUIDE

Likelihood	a	b	c	d	e
e	**M**	**M**	**H**	**H**	**H**
d	**L**	**M**	**M**	**H**	**H**
c	**L**	**L**	**M**	**M**	**H**
b	**L**	**L**	**L**	**M**	**M**
a	**L**	**L**	**L**	**L**	**M**

Consequence (a–e)

RISK ASSESSMENT

R HIGH – Unacceptable. Major disruption likely. Different approach required. Priority management attention required.

Y MODERATE – Some disruption. Different approach may be required. Additional management attention may be needed.

G LOW – Minimum impact. Minimum oversight needed to ensure risk remains low.

Level	Technical Performance	and/ or	Schedule	and/ or	Cost	and/ or	Impact on Other Teams
a	Minimal or no impact		Minimal or no impact		Minimal or no impact		None
b	Acceptable with some reduction in margin need dates		Additional resources required; able to meet		<5%		Some impact
c	Acceptable with significant reduction in margin		Minor slip in key milestones; not able to meet need date		5-7%		Moderate impact
d	Acceptable; no remaining margin		Major slip in key milestone or critical path impacted		7-10%		Major impact
e	Unacceptable		Can't achieve key team or major program milestone		>10%		Unacceptable

Figure A-4. Risk Assessment Process

Probability/Likelihood. For each risk area identified, the probability/likelihood the risk will happen must be determined. As shown in Figure A-4, there are five levels (a-e) in the XYZ risk assessment process, with the corresponding subjective criteria of *Remote, Unlikely, Likely, Highly Likely*, and *Near Certainty*. If there is zero probability/likelihood of an event, by definition there is no risk.

Consequence/Impact. For each risk area identified, the following question must be answered: *Given the event occurs, what is the magnitude of the consequence/impact?* As shown in Figure A-4, there are five levels of consequence/impact (a-e). "Consequence/impact" is a multifaceted issue. For this project, there are four areas that will be evaluated when determining consequence/impact: technical performance, schedule, cost, and impact. At least one of the four consequence/impact areas needs to apply for there to be risk; if there is no adverse consequence/impact in any of the areas, there is no risk.

- Technical Performance: This category includes all requirements that are not included in the other three metrics of the Consequence/Impact table. The wording of each level is oriented toward design processes, production processes, life cycle support, and to retirement of the system. For example, the word "margin" could apply to weight margin during design, safety margin during testing, or machine performance margin during production.
- Schedule: The words used in the Schedule column, as in all columns of the Consequence/Impact table, are meant to be universally applied. Avoid excluding a consequence/impact level from consideration just because it doesn't match specific definitions.
- Cost: Since costs vary from component to component and process to process, the percentage criteria shown in Figure A-4 may not strictly apply at the lower levels of the WBS. These IPT can set the percentage criteria that best reflects the situation. However, when costs are rolled up at higher levels, the following definitions will be used: Level 1 – no change, Level 2 – <5%, Level 3 – 5 to7%, Level 4 – 7 to10%, and Level 5 – >10%.
- Impact on Others: Both the consequence/impact of a risk and the mitigation actions associated with reducing the risk may impact other projects or organizations. This may involve additional coordination or management attention (resources) and may therefore increase the level of risk. This is especially true of common technical processes.

Risk Rating. Probability and consequence/impact should not always be considered equally. For example, there may be consequences/impacts so severe that they are considered high risk even though the probability to achieve a particular outcome is low. After deciding a level of process variance/probability/likelihood (a through e) and a level of consequence/impact (a through e), enter the *Assessment Guide* portion of Figure A-4 to obtain a risk rating (green = LOW, yellow = MOD, and red = HIGH). For example; consequence/impact/process variance/probability/likelihood level 2b corresponds to LOW risk, level 3d corresponds to MOD risk, level 5c corresponds to HIGH risk. After obtaining the risk rating, make a subjective comparison of the risk event with the applicable rating definition in Figure A-4 (e.g., High = unacceptable, major disruptions, etc.). There should be a close match. If there isn't, consider reevaluating the level of probability/likelihood or consequence/impact. Those risk events that are assessed as moderate or high should be submitted to the XYZ Risk Management Coordinator on a Risk Information Form.

Figure A-4 is useful to convey information to decision-makers and will be used primarily for that purpose. The PD/PM will use the Risk Tracking Report and Watch List.

3.4 Risk Handling

3.4.1 Process

After the project's risks have been identified and assessed, the approach to handling each significant risk must be developed. There are essentially four techniques or options for handling risks: avoidance, control, transfer, and assumption. For all identified risks, the various handling techniques should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, and the effect on the system's technical performance, and the most suitable technique selected. The results of the evaluation and selection will be included and documented in the Risk Management Information System using the Risk Information Form. This documentation will include: what must be done, the level of effort and materials required, the estimated cost to implement the plan, a proposed schedule showing the proposed start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant project activities/milestones, recommended metrics for tracking the action, a list of all assumptions, and the individual responsible for implementing and tracking the selected option.

3.4.2 Procedures

The IPT is responsible for evaluating and recommending to the PD/PM the risk-handling options that are best fitted to the project's circumstances. Once approved, these are included in the project's acquisition strategy or management plans, as appropriate.

For each selected handling option, the IPT will develop specific tasks that, when implemented, will handle the risk. The task descriptions should explain what has to be done, the level of effort, and identify necessary resources. It should also provide a proposed schedule to accomplish the actions including the start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant project activities/milestones, and a cost estimate. The description of the handling options should list all assumptions used in the development of the handling tasks. Assumptions should be included in the Risk Information Form. Recommended actions that require resources outside the scope of a contract or official tasking should be clearly identified, and the IPTs, the risk area, or other handling plans that may be impacted should be listed.

Reducing requirements as a risk avoidance technique should be used only as a last resort, and then only with the participation and approval of the user's representative.

3.5 Risk Monitoring

3.5.1 Process

Risk monitoring systematically tracks and evaluates the performance of risk-handling actions. It is part of the project management function and responsibility and should not become a separate discipline. Essentially, it compares predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk-handling actions. The effectiveness of the risk-monitoring process depends on the establishment of a management indicator system (metrics) that provides accurate, timely, and relevant risk information in a clear, easily understood manner. The metrics selected to monitor project status must adequately portray the true state of the risk events and handling actions. Otherwise, indicators of risks that are about to become problems may go undetected.

To ensure that significant risks are effectively monitored, risk-handling actions (which include specific events, schedules, and “success” criteria) will be reflected in integrated project planning and scheduling. Identifying these risk handling actions and events in the context of Work Breakdown Structure (WBS) elements establishes a linkage between them and specific work packages, making it easier to determine the impact of actions on cost, schedule, and performance. The detailed information on risk-handling actions and events is included in the RIF for each identified risk, and thus is resident in the Risk Management Information System.

3.5.2 Procedures

The functioning of the IPT is crucial to effective risk monitoring. The IPT is the “front line” for obtaining indications that risk-handling efforts are achieving the desired effects. The IPT is responsible for monitoring and reporting the effectiveness of the handling actions for the risks assigned. Overall XYZ project risk assessment reports will be prepared by the XYZ Risk Management Coordinator working with the IPT.

Many techniques and tools are available for monitoring the effectiveness of risk-handling actions, and the IPT must ensure that they select those that best suit their needs. No single technique or tool is capable of providing a complete answer—a combination should be used. At a minimum, the IPT maintains a watch list of identified high priority risks.

Risks rated as Moderate or High risk will be reported to the XYZ Risk Management Coordinator, who tracks them, using information provided by the IPT, until the risk is considered Low and recommended for “Closeout.” The IPT retains ownership and cognizance for reporting status and keeping the database current. Ownership means implementing handling plans and providing periodic status of the risk and of the handling plans. Risk will be made an agenda item at each management or design review, providing an opportunity for all concerned to offer suggestions for the best approach to managing risk.

Communicating risk increases the project's credibility and allows early actions to minimize adverse consequences/impacts.

The risk management process is continuous. Information obtained from the monitoring process is fed back for reassessment and evaluations of handling actions. When a risk area is changed to Low, it is put into a "Historical File" by the Risk Management Coordinator and no longer tracked by the XYZ PD/PM. The "owners" of all Low risk continue monitoring Low risks to ensure they stay Low.

The status of the risks and the effectiveness of the risk-handling actions are reported to the Risk Management Coordinator:

- Quarterly
- When the IPT determines that the status of the risk area has changed significantly (as a minimum when the risk changes from high to moderate to low, or vice versa)
- When requested by the PD/PM.

4.0 Risk Management Information System and Documentation

The XYZ project will use the XXX database management system as its Risk Management Information System. The system will contain all of the information necessary to satisfy the project documentation and reporting requirements.

4.1 Risk Management Information System

The Risk Management Information System stores and allows retrieval of risk-related data. It provides data for creating reports and serves as the repository for all current and historical information related to risk. This information will include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The PD/PM will use data from the Risk Management Information System to create reports for senior management and retrieve data for day-to-day management of the project. The project produces a set of standard reports for periodic reporting and has the ability to create ad hoc reports in response to special queries. See Attachment I for a detailed discussion of the Risk Management Information System.

Data is entered into the Risk Management Information System using the Risk Information Form. The Risk Information Form gives members of the project team, both DOE and contractors, a standard format for reporting risk-related information. The Risk Information Form should be used when a potential risk event is identified and is updated as information becomes available as the assessment, handling, and monitoring functions are executed.

4.2 Risk Documentation

All project risk management information will be documented, using the Risk Information Form as the standard Risk Management Information System data entry form. The following paragraphs provide guidance on documentation requirements for the various risk management functions.

4.2.1 Risk Assessment Documentation

Risk assessments form the basis for many project decisions. From time to time, the PD/PM will need a detailed report of any assessment of a risk event. It is critical that all aspects of the risk management process are documented.

4.2.2 Risk Handling Documentation

Risk-handling documentation will be used to provide the PD/PM with the information he needs to choose the preferred mitigation option.

4.2.3 Risk Monitoring Documentation

The PD/PM needs a summary document that tracks the status of high and moderate risks. The Risk Management Coordinator will produce a risk tracking list, for example, that uses information that has been entered from the Risk Management Information System. This document will be produced on a monthly basis.

4.3 Reports

Reports are used to convey information to decision-makers and team members on the status of the program and the effectiveness of the risk management program. Every effort will be made to generate reports using the data resident in the Risk Management Information System.

4.3.1 Standard Reports

The Risk Management Information System will have a set of standard reports. If the IPT or functional managers need additional reports, they should work with the Risk Management Coordinator to create them. Access to the reporting system will be controlled; however, any member of the Government or contractor team may obtain a password to gain access to the information.

4.3.2 *Ad Hoc* Reports

In addition to standard reports, the PD/PM will need to create ad hoc reports in response to special queries. The Risk Management Coordinator will be responsible for these reports.

Attachment I
To XYZ Risk Management Plan--
Management Information System and Documentation

1.0 Description

In order to manage risk, a database management system is needed that stores and allows retrieval of risk-related data. The Risk Management Information System provides data for creating reports and serves as the repository for all current and historical information related to risk. This information may include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The Risk Management Coordinator is responsible for the overall maintenance of the Risk Management Information System, and he or his designee are the only persons who may enter data into the database.

The Risk Management Information System will have a set of standard reports. If the IPT or functional managers need additional reports, they should work with the Risk Management Coordinator to create them. Access to the reporting system will be controlled; however, any member of the DOE or contractor team may obtain a password to gain access to the information.

In addition to standard reports, the PD/PM will need to create ad hoc reports in response to special queries etc. The Risk Management Coordinator will be responsible for these reports. Figure I-1 shows a concept for a management and reporting system.

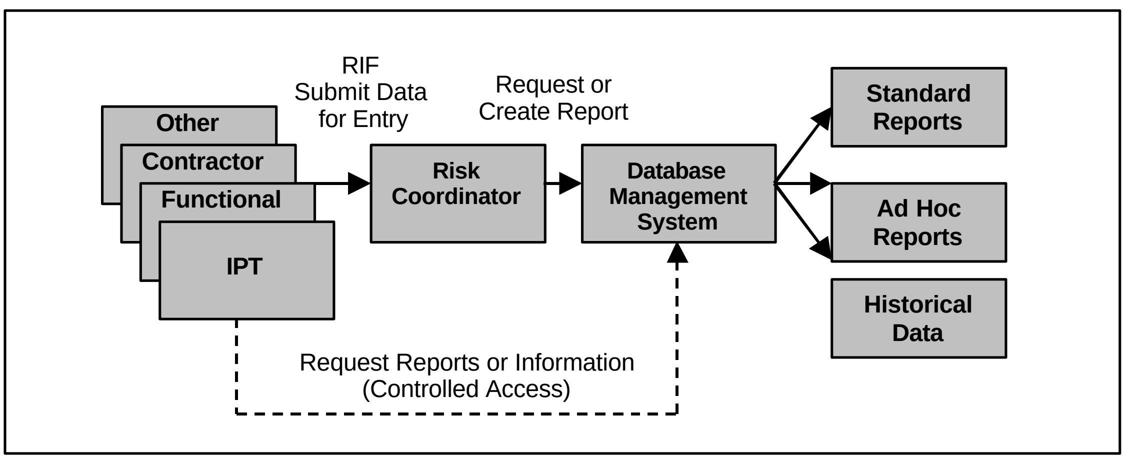


Figure I-1. Risk Management Concept

2.0 Risk Management Reports—XYZ Program

Following are examples of basic reports that a PD/PM may use to manage the risk program. Each user should coordinate with the Risk Management Coordinator to tailor and amplify reports, if necessary, to meet specific needs.

2.1 Risk Information Form

The PD/PM needs a document that serves the dual purpose of a *source* of data entry information and a *report* of basic information for the IPT, etc. The Risk Information Form serves this purpose. It provides members of the project team, both DOE and contractors, a format for reporting risk-related information. The Risk Information Form should be used when a potential risk event is identified and updated as information becomes available and the status changes. As a source of data entry, the Risk Information Form allows the database administrator to control entries. The format for a Risk Information Form is shown in Figure I-2.

Risk Information Form	
Risk Identification Number Risk Event: Priority	Date
Major System/Component/Functional Area: Category: Statement of Risk:	
	Description of Risk:
	Key Parameters: Assessment:
	Analysis:
	Process Variance Probability of Occurrence: Consequence:
Time Sensitivity: Other Affected Areas:	
Risk Handling Plans:	
Risk Monitoring Activity:	
Status	
	Status Date:
Assignment:	Reported By:

Figure I-2. Risk Information Form

2.2 Risk Assessment Report

Risk assessments form the basis for many project decisions, and the PD/PM may need a detailed report of assessments of a risk event that has been completed. A Risk Assessment Report is prepared by the entity that assessed a risk event and amplifies the information in the Risk Information Form. It documents the identification, analysis, and handling processes and results. The Risk Assessment Report amplifies the summary contained in the Risk Information Form, is the basis for developing risk-handling plans, and serves as a historical recording of project risk assessment. Since Risk Assessment Reports may be large documents, they may be stored as files. Risk Assessment Reports should include information that links them to the appropriate Risk Information Form.

2.3 Risk-Handling Documentation

Risk-handling documentation may be used to provide the PD/PM with information needed to choose the preferred mitigation option and is the basis for the handling plan summary contained in the Risk Information Form. This document describes the examination process for risk-handling options and gives the basis for the selection of the recommended choice. After the PD/PM chooses an option, the rationale for that choice may be included. There should be a time-phased plan for each risk-mitigation task. Risk-handling plans are based on results of the risk assessment. This document should include information that links it to the appropriate Risk Information Form.

2.4 Risk Monitoring Documentation

The PD/PM needs a summary document that tracks the status of high and moderate risks. The XYZ project will use a risk-tracking list that contains information that has been entered from the Risk Information Form. An example of the tracking report/list is shown in Table I-1.

Table I-1. Risk Tracking Report Example

I.	Risk Area Status: Design		P_F: Hi	C_F: Hi
	Significant Design Risks:			
	1. Title: System Weight		P_F: Hi	C_F: Hi
	Risk Event:	Exceed system weight by 10%; increasing facility size and energy		
	Action:	Examining subsystems to determine areas where weight may be reduced. Reviewing the requirement. Closely watching the effect on reliability and survivability.		
	2. Title: Design Analysis		P_V: Hi	C_V: Hi
	Risk Event:	Failure Modes, Effects and Criticality Analysis (FMECA) is planned too late to identify and correct any critical single-point failure points prior to design freeze.		
	Action:	Additional resources are being sought to expedite performance of FMECA.		
II.	Risk Area Status: Supportability		P_F: Hi	C_F: Mod/Hi
	1. Title: Operational Support		P_F: Hi	C_F: Mod/Hi
	Risk Event:	Vessel subcontractor is in financial trouble and may go out of business. No other known sources exist.		
	Action:	Doing trade study to see if alternative designs have a broader vessel supply vendor base. Prime contractor is negotiating with the subcontractor to buy drawings for development of second source.		

3.0 Database Management System

The XYZ Risk Management Information System provides the means to enter and access data, control access, and create reports. Key to the Management Information System are the data elements that reside in the database. Listed in Table I-2 are the types of risk information that will be included in the database. “Element” is the title of the database field; “Description” is a summary of the field contents. The Risk Management Coordinator will create the standard reports such as, the Risk Information Form, Risk Monitoring, etc. The Risk Management Information System also has the ability to create “ad hoc” reports, which can be designed by users and the Risk Management Coordinator.

Table I-2. DBMS Elements

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PD/PM. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PD/PM compared to all other risks, e.g., a one (1) indicates the highest priority.
Data Submitted	Gives the date that the RIF was submitted.
Major System/ Component	Identifies the major system/component based on the WBS.
Subsystem/Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) of the risk.
Description of Risk	Briefly describes the risk. Lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, includes how it is manifested (e.g., design and engineering, manufacturing, etc.)
Key Parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report, if appropriate.
Analyses	Briefly describes the analysis done to assess the risk. Includes rationale and basis for results.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the project's Risk Management Plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the project's Risk Management Plan.
Time Sensitivity	Estimates the relative urgency for implementing the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measures using metrics for tracking progress in implementing risk handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk handling milestones.
Status Due Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

4.0 Watch List

Risk elements that should be given special management attention are often entered into PD's/PM's risk watch list. Each element on the watch list is fully identified, along with risk action plans, action code, due date and complete date, and if desired, a responsible individual.

Table I-3. Watch List Example

Potential Risk Area	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
• Accurately predicting seismic environment equipment will experience.	• Use multiple finite element codes & simplified numerical models for early assessments. • Seismic test simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SE03 SE03	31 Aug 01 31 Aug 02		
• Evaluating impact of the facility systems that are not similar to previous designs.	• Concentrate on modeling and scale testing of technologies not demonstrated successfully in large-scale tests or full-scale trials.	SE031	31 Aug 01		