

***MILITARY SPECIFICATIONS AND STANDARDS  
REFORM PROGRAM (MSSRP)***

---

**CRITICAL PROCESS ASSESSMENT TOOL  
(CPAT)**

***RISK MANAGEMENT***

**14 August 1998**

**SMC/AXD**

# Critical Process Assessment Tool (CPAT)

## Risk Management

<b>SECTION 1. INTRODUCTION</b> .....	<b>3</b>
1.1 Description of the Risk Management Critical Process.....	4
1.2 Contribution to Mission Success .....	5
1.3 Relationship to Other Technical Tasks.....	5
1.4 Definitions .....	6
1.5 Applicable Documents.....	7
1.6 Additional Support.....	8
<b>SECTION 2. RFP SUPPORT</b> .....	<b>9</b>
2.1 Critical Process Objectives for Inclusion in the Statement of Objectives .....	9
2.2 Data Deliverables.....	10
2.2.1 CDRLs and the Data Accession List .....	10
2.2.2 Data Accession List and Other Data.....	10
2.3 Proposal Preparation Instructions (Section L) .....	10
2.4 Evaluation Criteria (Section M) and Standards .....	11
2.4.1 Evaluation Criteria (Section M).....	11
2.4.2 Source Selection Standards .....	12
<b>SECTION 3. CRITICAL PROCESS EVALUATION AND ASSESSMENT</b> .....	<b>14</b>
3.1 Technical Evaluation and Review Questions .....	14
3.2 Risk Trigger Questions .....	16
<b>ANNEX 1 GLOSSARY</b> .....	<b>20</b>
<b>ANNEX 2 ACRONYMS</b> .....	<b>22</b>
<b>ANNEX 3 SOME ASPECTS OF THE RISK MANAGEMENT PROCESS</b> .....	<b>23</b>

# Critical Process Assessment Tool (CPAT)

## Risk Management

### Section 1. Introduction

The Critical Process Assessment Tools (CPATs) support project officers and project engineers (1) in preparing Requests for Proposals (RFPs), (2) in preparing for the subsequent source selection (for competitive procurements) or Tech Eval and Fact finding (for non-competitive contract actions), and (3) in preparing to participate in or review contract execution after contract award. The CPATs are applicable to processes that are considered to be critical to the execution of the contract.

This version of the CPAT, called the **Risk Management CPAT**, provides support for the risk management process. To use this CPAT, you should first review the separate **CPAT Overview and Program Management CPAT**, then this **Risk Management CPAT**. The Overview CPAT provides a description of the tool's format, guidance on its usage, and an overview of the acquisition process, so it should be consulted by the first time reader. It does not provide any directly applicable critical process information. The Program Management, Systems Engineering, and Risk Management CPATs contain specific process information that provides top down direction to the other CPATs. These are the functions that are common to and inherent in the execution of any process.

The following table is a road map to the Risk Management CPAT.

If you want support in the following:	Then do the following:.
An <b>overview</b> of the risk management critical process.	Read Sections 1.1 and 1.3, referring to Annex 1 for definitions of unfamiliar terms. If a more thorough introduction is desired, then refer to Annex 3 or the documents listed in Section 1.5.
Prepare the risk management inputs for the development of an <b>RFP</b> .	<ol style="list-style-type: none"> <li>1. Review Sections 1.1 to 1.6 for background.</li> <li>2. Review the road map to RFP preparation support at the beginning of Section 2.</li> <li>3. To develop <b>risk management objectives</b> for incorporation into the overall RFP <b>Statement of Objectives (SOO)</b>, <b><u>tailor</u></b> the objectives in the subsection of 2.1 corresponding to the program phase for which you're preparing</li> <li>4. To define <b>data items</b> that are pertinent to risk management and are to be required by the RFP, apply Section 2.2.</li> <li>5. To develop <b>proposal preparation instructions</b> that serve as a starting point for RFP <b>Section L</b>, start with Section 2.3.</li> <li>6. To prepare risk management inputs for a <b>Glossary</b> and <b>list of acronyms</b> for incorporation as attachments to RFP Section J, see Annex 1 and Annex 2.</li> <li>7. To develop <b>source selection criteria</b> pertinent to risk management for incorporation into RFP Section M, apply Section 2.4.1.</li> </ol>
Prepare risk management inputs to the <b>source selection standards</b> .	<b><u>Tailor</u></b> the standards in Section 2.4.2. <b><u>The tailoring should account for the latest policy for preparing both the standards and the objectives related to risk management to be included in the SOO in the RFP or reflected in the factors or assessment criteria in Section M.</u></b>
Prepare for a non-competitive Technical Evaluation ( <b>Tech Eval</b> ) and <b>Factfinding</b> .	Apply the questions in Section 3.1.
Maintain <b>insight</b> into the contractor's progress in risk management after contract award.	Apply the questions in Section 3.1 and 3.2.

## 1.1 Description of the Risk Management Critical Process

Risk Management is an integral part of the systems engineering process and the overall program management effort. The need for risk management is mentioned in several DoD directives, initiatives, and associated documents, as discussed in Section 1.5. Risk management supports a variety of program acquisition documents and activities, including the Integrated Program Summary (IPS), CAIV, and milestone exit criteria.

Risk management is the act or practice of controlling risks that have a potential for causing unwanted program impacts. This process includes: planning a structured approach (risk planning), identifying and analyzing risk items and areas (risk assessment), developing risk handling plans (part of risk handling) and monitoring risk handling activities to determine how risks have changed (risk monitoring).

Several tools are available to assist the program office in understanding the danger signals that may indicate the program is off-track, determining the seriousness of the problem, and prioritizing corrective actions as necessary. Risk management is not a separate program office activity assigned to a risk management branch, but rather is one aspect of a sound systems engineering and technical management program.

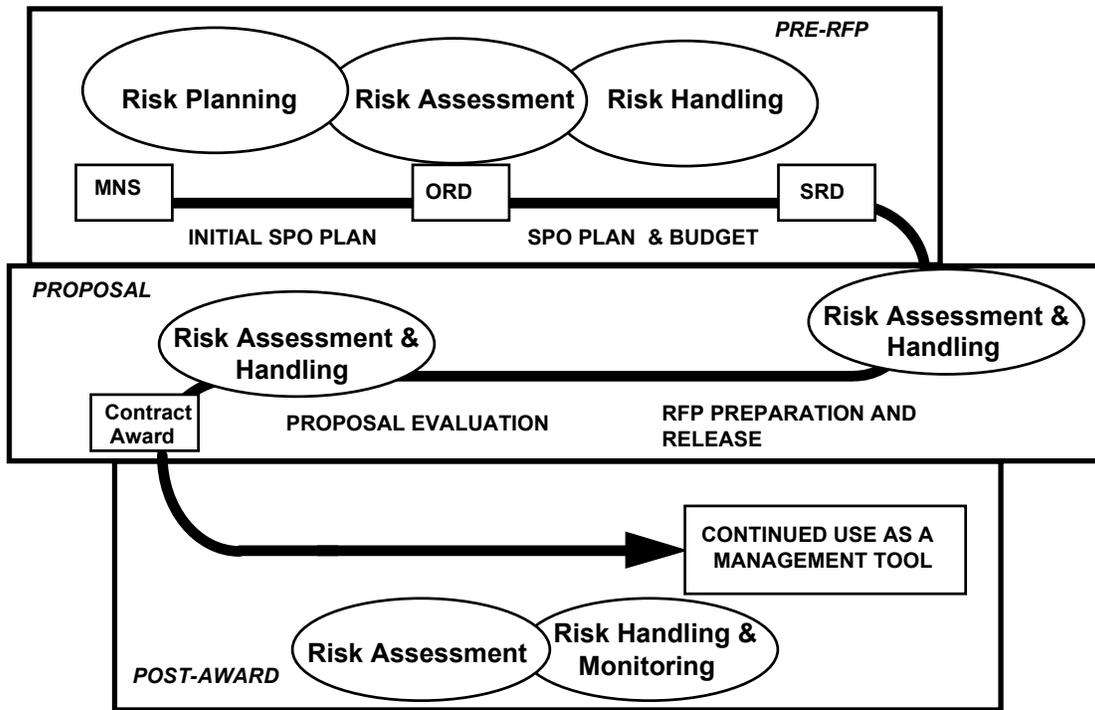
“Risk Management” is the “umbrella” title for the processes used to manage risk. There are four main facets of the risk management process, as given by the risk management process promulgated by the Office of the Secretary of Defense (OSD), including: (1) risk planning, (2) risk assessment (both identification and analysis), (3) risk handling and (4) risk monitoring. A simplified flow of how the risk management process is implemented in a program is given in Figure 1. (The risk management process, including risk planning, assessment, handling and monitoring functions, is discussed in detail in Annex 3.) An ultimate goal of the risk management process is to identify and evaluate program risks, and develop and implement a suitable risk handling plan to mitigate these risks.

Four basic actions must be taken to effectively assess a program’s risk. First, as part of the risk planning process, the government or contractor program office should establish the basic approach it will use to assess the risks and the working structure for the risk assessment. Second, as part of the risk assessment process, the government or contractor program office should identify and analyze the risks in the program. Third, as part of the risk handling process, suitable risk handling strategies should be developed and enacted. Fourth, as part of the risk monitoring process, the performance of risk handling actions is systematically tracked and evaluated against established metrics throughout the acquisition process.

The risk management process is needed throughout the defense program acquisition cycle. It is important that a risk management strategy be established early in a program (during the Concept Exploration and Definition Phase) and that risk be continually addressed throughout the system life cycle. The process should be performed on a somewhat regular basis, such as a major review conducted once a year with updates as needed (e.g., quarterly), in addition to material required to support major program milestones and reviews (e.g., incorporated in the IPS).

The risk management process does not fundamentally change as the program matures. What will vary during the course of the program is an increasing level of refinement associated with: (1) inputs to the risk management process, (2) the risk assessment methodology and (3) implementation of the individual process functions. This is particularly true for risk assessment and risk handling activities.

The risk management process should examine potential risks to the program ground, launch, and space segments (as applicable). At a minimum, the risk management process should examine cost, performance and schedule (C,P,S) risk areas. Other potentially important risk areas may exist for a given program and should be similarly identified and examined. (For example, this may include funding (budget) risk for some programs.) The risk management process should evaluate both hardware, software and integration items. It should also be performed at an appropriate PWBS level to ensure that key risk items are indeed identified and tracked.



**Risk Management During the Acquisition Process**  
**Figure 1**

## 1.2 Contribution to Mission Success

Unless a disciplined, comprehensive risk management process is implemented, program risks may not be adequately identified nor a suitable risk handling plan be developed and implemented. Inadequate or ineffective risk management can result in cost increases, schedule slips, and products or systems that cannot meet performance goals or may be impractical to build. Risk management will be particularly critical to the success of a program when high performance levels are required and the design approaches or exceeds the existing state of the art. The need for an effective risk management process is made all the more important when a potentially inadequate program budget and/or schedule exists.

The “cost” associated with lost opportunities from inadequate risk management may be high. A high opportunity “cost” may result when problems are identified late in the program that could otherwise have been solved earlier through a proactive risk management process. This is because the ability to readily resolve major hardware and software problems is usually limited late in a program since: (1) a substantial investment has already been made with the chosen design; (2) funding is limited and the schedule is constrained; and (3) C,P,S cannot be perfectly traded in the short-run. The need for major redesigns late in a program can often be reduced or avoided by implementing a sound risk management process. (Of course, externally mandated changes (e.g., budget or requirements) can adversely affect any program, and are often beyond the control of the program.)

## 1.3 Relationship to Other Technical Tasks

The concept of risk management should not be treated as a separate program entity or added-on function, but is an integral part of the overall program planning and management process to aid the program office in developing options and making smart decisions to control the outcome of events.

The risk management process is also a fundamental part of the overall program systems engineering and program management processes. For example, risk management may be viewed as being part of the systems engineering systems analysis and control function, which measures progress, evaluates alternatives, selects

preferred alternatives, and documents data used and generated. Other key systems analysis and control functions that can interact with the risk management process include: trade-off studies, system/cost effectiveness analysis, life cycle cost analysis, configuration management, interface management, data management, systems engineering master schedule, technical performance measurement (TPM), and technical reviews. (For example, TPMs are a key means for monitoring potential risk reduction progress.)

As previously mentioned in Section 1.1, the risk management process does not fundamentally change as the program matures. Of course, as the program matures additional information relating to the individual risk areas will become available from a variety of sources (e.g., design changes, experiments, technology demonstrations, process developments, etc.) and should be incorporated into the risk management process. The risk management process is not a static one, but continued through the life of the program. It should be used in a proactive manner to both identify and evaluate risk areas and candidate risk handling approaches, as well as to monitor the progress of the selected risk handling approaches.

Some degree of risk always exists in logistics, manufacturing, program and technical areas. Logistics risks associated with user suitability include: reliability, maintainability, operability, and trainability concerns. Manufacturing risk includes concerns over: quality, rework, producibility, packaging, lead times, and material availability. Program risks include: funding, schedule, contract relationships, and political risks. Technical risks may involve the risk of meeting a performance requirement such as reliability, probability of first weapon hit, maneuverability or survivability, but may also involve risks in the feasibility of a design concept or the risks associated with using state-of-the-art equipment or software. The understanding of risks in these and other areas evolves over time. Consequently, risk management should span the range of program functions and continue throughout the program's life cycle.

Risk management documentation should be maintained and updated during the course of the program. This will help provide a record of inputs to key decisions, decisions made, lessons learned, etc. It will also provide suitable risk assessment and risk planning information that is necessary as part of the Integrated Program Summary (IPS) required for program milestone reviews. The level and scope of risk management documentation will vary somewhat during the course of the program, likely being the most extensive in the Dem/Val through EMD program phases. The risk management documentation will also likely be most extensive in the risk analysis and risk handling areas for most programs.

Other key systems analysis and control functions that can interact with the risk management process include: trade-off studies, system/cost effectiveness analysis, configuration management, interface management, data management, and technical performance measurement. The Cost as an Independent Variable (CAIV) process is also strongly related to the risk management process and it requires a strong risk management process to be successfully implemented.

The risk management process does not fundamentally change as the program matures. Of course, as the program matures, additional information relating to the individual risk areas will become available from a variety of sources (e.g., design changes, experiments, technology demonstrations, process developments, budget changes, etc.) and should be incorporated into the risk management process. The risk management process is not static, but continues throughout the life of the program. It should be used in a proactive manner to identify and evaluate risk areas and candidate risk handling approaches, as well as to monitor the progress of the program in response to selected risk handling approaches.

## **1.4 Definitions**

See Annex 1 for a glossary of program management and related terms used in this CPAT.

See Annex 2 for a list of acronyms.

## 1.5 Applicable Documents

Document	Discussion	Source
DoD Directive 5000.1, "Defense Acquisition," 15 March 1996, Section D.1.d.	Outlines the need to implement a suitable risk management process and to use it continuously. The ability of a program to transition into the next phase of the acquisition process will depend upon risks being understood and risk management approaches developed.	Defense Acquisition Deskbook, Version 2.3; OSD (A&T) and other World Wide Web (WWW) sites; the SMC library or The Aerospace Corporation library.
DoD 5000.2-R "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," 15 March 1996, Sections 3.3.2 and 4.3.	Covers cost, schedule, and performance risk management (Section 3.3.2) and systems engineering risk management (Section 4.3). Section 3.3.2 outlines characteristics of the risk management process to be implemented and the relationship to the design process. Section 4.3 outlines the need to establish a risk management process for use throughout the design process and how technical risks are to be identified and evaluated as part of systems engineering.	Defense Acquisition Deskbook, Version 2.3, OSD (A&T) and other World Wide Web (WWW) sites, the SMC library or The Aerospace Corporation library.
Defense Acquisition Deskbook, Version 2.3, 15 March 1998.	Includes OSD risk management process contained within the Deskbook's Information Structure Files.	Defense Acquisition Deskbook Office, (Dayton, Ohio) or their WWW site.
"Risk Management Guide," Defense Systems Management College, March 1998.	The entire document is devoted to various aspects of risk management. It has been completely re-written versus the previous release (March 1989) to reflect enhanced risk management practices and processes and is in complete alignment with the OSD risk management process.	Defense Systems Management College Press (Ft. Belvoir, Virginia).
"Acquisition Risk Management Guide," AFMC Pamphlet 63-101, 7 July 1997.	This pamphlet is a reference that outlines Air Force Materiel command's approach to implementing DoD risk management policy. It has been completely re-written versus the previous release (September 1993) to reflect enhanced risk management practices and processes and is in complete alignment with the OSD risk management process. Another re-write is currently under way to correct identified deficiencies (e.g., mathematics on ordinal risk scales).	AFMC (Dayton, Ohio) or their WWW site.
"Improving Risk Communication," National Research Council, National Academy Press, 1989.	This book is devoted to discussing the process of risk communication, the content of risk messages, and ways to improve risk communication. (The book does not, however, provide a set of detailed guidelines and is not a "how-to" manual for risk communicators.)	National Research Council (Washington, D. C.).

<p>Lloyd K. Mosemann, "Guidelines for Successful Acquisition and Management of Software Intensive Systems," Version 2-- Volume 1, June 1996.</p>	<p>Several sections of this document contain material relevant to risk management, including Chapter 6 (Risk Management), plus portions of Chapters 3 (Systems Life Cycle and Methodologies), 12 (Strategic Planning), 13 (Contracting for Success) and 16 (The Challenge). The material presented generally applies to both hardware and software items.</p>	<p>Air Force Software Technology Support Center (Hill AFB, Utah) or their WWW site. Note: the size of all 35 compressed files in this document is 9.5 MB and the decompressed size is approximately 40 MB. Consider downloading just those files corresponding to the referenced chapters.</p>
--	---	--

## 1.6 Additional Support

Contact SMC/AXD at LAAFB, (310) 363-0131 for additional support and the latest policies on risk management. If he is unavailable, call 363-2036 for assistance. (The corresponding DSN is 833-XXXX.)

## Section 2. RFP Support

The previous section provided an introduction to the risk management process for defense acquisition programs as a prelude to providing specific support to project officers and project engineers. A road map to the support for preparing Requests for Proposals (RFPs) is in the following table.

<b>RFP Element</b>	<b>Program Management Project Officer &amp; Project Engineer role</b>	<b>Section below where support is given</b>
Statement of Objectives	Recommend risk management objectives for inclusion in the RFP SOO	2.1
Data Deliverables	Recommend risk management data requirements to be included in the RFP	2.2
Proposal Preparation Instructions (PPI) in Section L	Recommend instructions that are pertinent to risk management and, in some cases, all the critical processes and that serve as a starting point for developing the PPI	2.3
Evaluation Factors for Award, Section M	Recommend risk management Evaluation Factors and Sub-factors	2.4
Glossary of terms and List of Acronyms used In the RFP, to be included as an attachment listed in Section J or in some other way	Identify risk management terms to be included in the Glossary and List of Acronyms	Annex 1 and Annex 2, respectively

In the case of **competitive procurements**, the Government also prepares **standards** to be used in the source selection process. Support to the project officer and project engineer in preparing standards is given in Section 2.4.

Support for preparing **technical evaluations** (Tech Evals) for **non-competitive procurements** and for participating in or reviewing contractor activities after contract award is provided later in Section 3.1 and 3.2.

### 2.1 Critical Process Objectives for Inclusion in the Statement of Objectives

A risk management process is needed throughout the program’s life cycle. At a minimum, adequate risk planning, assessment (identification and analysis), handling and monitoring must be accomplished. (See Annex 3 of this CPAT for additional information.) However, the types of risks and the acceptable level of risk for an item, and thus the program’s risk management objectives, will vary somewhat between program phases as well as between programs. Key guidance for risk management across the length of a program is given in DoDD 5000.1 (Section D.1.d) and DoD 5000.2-R (Sections 3.3.2 and 4.3 ), plus the OSD risk management process given in the Defense Acquisition Deskbook.

**In preparing a SOO, the objective presented here should be tailored to account for both the latest policy for preparing the SOO and the specific scope and risks of the contract you are planning.**

**Objective:**

Develop and implement a risk management process with risk planning, assessment (identification and analysis), handling, and monitoring functions. In addition, as appropriate, add: “Establish quantified acceptable risk levels to be achieved prior to transitioning to the next program phase.”

## 2.2 Data Deliverables

### 2.2.1 CDRLs and the Data Accession List

Current policy is to minimize the number and cost of CDRL items required by the contract to those directly required by policy or essential because of program risk. For risk management, it is recommended that a Risk Management Plan (RMP) be prepared and that it be maintained and updated throughout the life of the contract. The RMP should be specified in Form 1423 (CDRL) to include:

- The contractor's risk management process (including risk planning, assessment (identification and analysis), handling and monitoring activities).
- How risk management is implemented in the contractor's organization.
- How risk management is integrated into the contractor's systems engineering and program management processes.
- How risk management is implemented into the contractor's program review process.
- Risk management ground rules and assumptions (used for risk assessment and handling).
- Risk assessment (identification and analysis) methodology.
- Forms used for documenting risk identification, analysis, handling and monitoring activities.
- Results of a comprehensive risk assessment (performed once a year), risk handling plans for all items judged to be medium and high risk, corresponding risk monitoring metrics for these risk items, and results to date in resolving these risk issues.

### 2.2.2 Data Accession List and Other Data

The following data should be available through the data accession list or accessed through electronic sharing of program information: a) current definitions for risk levels, risks currently being tracked, risk handling plans and current status of these plans, minutes from review process (evidence that the process is ongoing), any risks identified that are to be evaluated and worked in an upcoming phase, and progress against risk milestones integrated into the IMS. When risk analyses are performed to quantify the uncertainty in key metrics such as cost, schedule, weight, or power, the results of these analyses should also be accessible.

See Section 2.4 of the Program Management CPAT for additional information on Data Accession Lists and Other Data, establishing access to contractor maintained data / databases, as well as, electronic data delivery.

## 2.3 Proposal Preparation Instructions (Section L)

RFP Section L or L-2 provides Proposal Preparation Instructions (PPI) to the contractors or offerors. To make the instructions given here as concise as practical, several risk management terms are used that are defined in Annex 1 of this CPAT. It is recommended that a glossary be included in the RFP.

The Program Management (Global) CPAT provides support that extends across all the critical processes. **This CPAT provides support specific to risk management for the following parts of the proposal:**

- The technical and/or management proposal or presentation, to the extent required by the RFP,
- Contract Data Requirements List (CDRL, if required),
- Other Data Items, if required,

- The Integrated Master Plan (IMP) or equivalent and
- Relevant Past/Present Performance.

The instructions developed using the following suggestions should be merged with those for the other critical processes, such as system engineering and program management. Instructions that may be directly copied and **tailored** to an RFP are in *italics*. **The tailoring should account for both the current policy on RFP preparation as well as the scope and objectives of your program.** Note also that when words such as “you” and “your” appear below in italics, they refer to the contractor.

***Technical and/or management proposal or presentation.*** Describe your risk management process, including risk planning, assessment (identification and analysis), handling, and monitoring functions. Describe your process for incorporating potential risk-driven impacts into proposal price, life cycle cost, and schedule. Describe how the risk management process is related to the systems engineering and program management processes. Describe your risk assessment (identification and analysis) methodology. Identify all medium or high risk items. Describe your risk handling approach, including option selected (assumption, avoidance, control or transfer), plus how you plan to implement it, for these medium and high risk items. Describe your proposed process including metrics for risk monitoring and how this information will be fed back to risk handling, analysis and identification activities. (Note to CPAT user: If program will be transitioning to a Dem/Val, EMD, or Production Phase on a subsequent contract, then the following additional instructions are suggested.) Define your approach to identifying and establishing quantified acceptable risk levels to be achieved prior to transitioning to the next program phase.

***Contract Data Requirements List (CDRL) (if preparation or extension by the contractor is to be required).*** Through an extension to the minimum CDRL (Note to CPAT User: delete “extension to the minimum CDRL” if a minimum CDRL is not included in the RFP) exhibit listed in Section J of the model contract, describe and commit to providing all risk management data requiring Government approval to include, as a minimum, the risk management plan.

***Other Data.*** Describe and commit in the CSOW or attachment to ready Government and other IPT member accessibility to risk management data to include, as a minimum: a) current definitions for risk levels, risks currently being tracked, risk handling plans and current status of these plans, minutes from review process (evidence that the process is ongoing), any risks identified that are to be evaluated and worked in an upcoming program phase, and progress against risk milestones integrated into the IMS. When risk analyses are performed to quantify the uncertainty in key metrics such as cost, schedule, weight, or power, the analysis results shall also be accessible.

***Integrated Master Plan (IMP) Narrative.*** (Note to the CPAT User: If the applicable objectives listed in Section 2.1 of this CPAT, appropriately **tailored**, are included in the SOO in the RFP, then it is recommended that you add the following to the overall instructions in the **Program Management CPAT** for the IMP and IMP Narrative:) ***Risk Management.*** Define the process(es) to be applied for carrying out the risk management objectives listed in the SOO.

***Relevant Past/Present Performance.*** If risk management is critical to the acquisition, then it is recommended that the following be added to the Section L instructions for the proposal section or volume on relevant past/present performance. ***Summarize the extent to which the risk management process committed to in the IMP was applied in the effort.***

## 2.4 Evaluation Criteria (Section M) and Standards

### 2.4.1 Evaluation Criteria (Section M)

The contractor’s description of the proposed processes, including the approach to the critical processes to control risk, and solution characteristics will be evaluated during source selection against the **evaluation criteria** in

Section M of the RFP. See the Program Management CPAT for a detailed discussion on source selection criteria and how they apply to the overall solicitation.

Generally, Risk Management is not identified as a stand alone Factor, but rather as a Sub-Factor or as a standard under a Factor or Sub-Factor. Assuming risk management is a Sub-Factor, items in *italics* may be directly copied and then tailored for use in an RFP (based on the current policy and the scope of your program) as follows:

*Sub-Factor: Risk Management*

## 2.4.2 Source Selection Standards

Once the proposals are received, they are compared to the source selection standards (not to each other). The information listed under each standard should be tailored to the solicitation.

**These suggested standards assume (1) that Section M of the RFP includes a single stand alone Sub-Factor Risk Management and (2) that the objectives from subsection 2.1 are incorporated into the SOO. If not, then the standards presented here must be tailored to correspond to Section M and the objectives.**

These standards also assume that corresponding suggested standards from the companion Program Management (Global) and System Engineering CPATs will be considered in preparing the complete set of standards for the source selection.

*STANDARD 1: RISK MANAGEMENT PROCESS. Describes an effective approach for risk management, including risk planning, assessment (identification & analysis), handling, and monitoring functions. The standard is met if:*

- a) The Offeror addresses how it will perform each function, and how the risk management process is integrated into the systems engineering and program management processes.*
- b) The Offeror addresses a list of risk management outputs to be generated and a description of each product.*
- c) The Offeror includes a schedule for performing the risk management process throughout the contract and describes how the schedule is linked to actions (e.g., assessments) and products.*
- d) The Offeror describes a risk management process that is linked with the program's IMP and IMS.*
- e) The Offeror addresses how the risk management process will be implemented at the prime contractor and major subcontractor levels, including roles and responsibilities of individual groups within each organization.*
- f) The Offeror addresses how the contractor will monitor the effectiveness of the risk management process, and how the government will access risk identification and risk analysis results, risk handling plans, schedules, and the status of risk handling activities.*

*STANDARD 2: RISK ASSESSMENT METHODOLOGY. Describes the risk assessment methodology for cost, performance and schedule risk that is appropriate and suitable for the specific design and technical management approach. The standard is met if:*

- a) The methodology is discussed in sufficient detail to permit evaluation of its suitability.*
- b) The Offeror addresses its approach for identifying potential risks at the system level and at lower WBS levels.*
- c) The Offeror addresses risk analysis associated with cost, schedule, and performance risk areas:
  - (1) that are likely to exist (e.g., technology risk),*
  - (2) for each system segment (e.g., space, ground and launch) and*
  - (3) for hardware, software and integration categories.**
- d) The Offeror described methodology that also covers other potential risk analysis areas that may be driven by other "requirements" imposed on the program (e.g., a computer security or a total system security risk assessment as part of threat risk assessment).*
- e) The methodology addresses both probability and consequence of occurrence components of risk, plus the time to initial impact.*

- f) *The Offeror does not attempt to perform mathematical operations on results obtained from uncalibrated (i.e., raw) probability and/or consequence of occurrence ordinal risk scales.*

*STANDARD 3: RISK IDENTIFICATION & ANALYSIS RESULTS. Describes the results of a comprehensive risk assessment performed against the specific design and proposed technical program management approach, using the methodology proposed by the Offeror. The standard is met if:*

- a) *The Offeror addresses risk assessment areas associated with cost, schedule, and performance:*
  - (1) *that are likely to exist (e.g., technology risk),*
  - (2) *for each system segment (e.g., space, ground and launch) and*
  - (3) *for hardware, software and integration categories.*
- b) *The Offeror addresses the ground rules and assumptions used in the risk assessment.*
- c) *The Offeror provides documentation of the ground rules and assumptions.*
- d) *The Offeror provides documentation of all items assessed as having medium or high cost, performance or schedule risk, including:*
  - (1) *a brief technical description of the item,*
  - (2) *risk analysis results and*
  - (3) *rationale discussing why the item possesses a medium or high risk level.*
- e) *Analysis and documentation of risk items addresses probability and consequence of occurrence components of risk, plus the time to initial impact.*
- f) *Information is provided in sufficient detail that the government evaluator can replicate the results for identified medium and high risk items given the methodology, and programmatic and technical descriptions of the items provided by the contractor.*

*STANDARD 4: RISK HANDLING AND RISK MONITORING APPROACH. Describes Risk Handling Plans and a risk monitoring approach that are effective and suitable for the proposed effort. The standard is met if the Offeror:*

- a) *Describes the risk handling option (assumption, avoidance, control, or transfer) for all items identified as medium or high risk.*
- b) *Addresses how suitable risk handling approaches will be identified, implemented and tracked with time for each medium or high risk item.*
- c) *Describes cost, performance, and schedule risk monitoring metrics to be used to track and evaluate the progress in reducing risk for each medium or high risk item.*
- d) *Addresses how the risk handling and risk monitoring processes are integrated with the program's IMS and IMP, including potential risk reduction and key program milestones.*
- e) *Addresses how the contractor will allocate resources against items identified as having medium or high risk.*
- g) *Addresses alternate concepts and / or designs along with cost, performance and schedule impacts to reduce the potential level of risk for each medium or high risk item.*

The following standard may only be appropriate when selecting sources for Concept Exploration and Definition, Dem / Val or Program Definition and Risk Reduction, and EMD contracts.

*STANDARD 5: RISK MANAGEMENT FOR TRANSITION. Describes how the approach to develop and provide quantified acceptable risk levels to be achieved prior to transition to the next acquisition phase. The standard is met if:*

- a) *The schedule for performing this activity is consistent with and supports the overall program and risk management schedule.*
- b) *The Offeror identifies all known significant risk areas critical to transition to the next acquisition phase and proposes to achieve quantifiable risk levels that are appropriate for entry into the next acquisition phase.*
- c) *The Offeror describes an approach which is cost effective, realistic, and achievable.*

## Section 3. Critical Process Evaluation and Assessment

The following list of questions associated with the objectives suggested in Section 2.3 are provided to: a) assist factfinding the risk management portion of non-competitive procurements, and b) to assist in post-award contract execution activities. In the case of post-award activities, it is expected that the project officer/engineer either participates in contractor/Government IPTs or in other ways reviews the contractor's progress, preferably in parallel with the contractors' activities. In addition, these questions assume that the contract requires an Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) or the equivalent.

Special care should be exercised to ensure that the contractor does not take these review questions as directing new contract scope. If the contractor personnel judge that a question reflects work outside the scope of the contract, then the matter should be reviewed with the Government Contracting Officer or the question should be tailored to the scope of the contract. **In particular, these review questions assume that the corresponding objectives in Section 2.1 were the basis for preparation of the Contract Statement of Work (CSOW), the IMP, or other equivalent compliance documents. If they were not, some of the work related to the questions may be outside the scope of the effort covered by the contract.**

### 3.1 Technical Evaluation and Review Questions

In addition to the objectives in Section 2.1 of this CPAT, the review questions presented in this section assume that a basic mission need has been defined in a Mission Need Statement (MNS) or Operational Requirements Document (ORD) and validated prior to the program phase addressed by the RFP. They also assume significant risk reduction steps (such as demonstrations and prototypes) will occur in the current or future acquisition phases. The questions should be tailored to be consistent with the scope of your program, the Proposal Preparation Instructions (Section L), and current acquisition policy.

#### **Obj.1. Develop and implement a risk management process with risk planning, identification, assessment, handling and monitoring functions.**

- RQ1. Has the contractor described its approach for risk management, including risk planning, assessment (identification and analysis), handling and monitoring functions?
- RQ2. Has the contractor described how it will implement each risk management function?
- RQ3. Has the contractor described how the risk management process is integrated into the systems engineering and program management processes?
- RQ4. Has the contractor provided a list of risk management outputs to be generated and a description of each product?
- RQ5. Has the contractor included a schedule for performing the risk management process during the phase and how the schedule is linked to actions (e.g., assessments) and products?
- RQ6. Has the contractor described how the risk management process is linked with the program's IMS and IMP?
- RQ7. Has the contractor described how the risk management process will be implemented at the prime contractor and major subcontractor levels, including roles and responsibilities of individual groups within each organization?
- RQ8. Has the contractor described how it will monitor the effectiveness of the risk management process, and how the government will access the risk identification and risk analysis results, risk handling plans, schedules and the status of risk handling activities?
- RQ9. Has the contractor developed and implemented an approach to provide suitable visibility for all items assessed as medium or high risk?
- RQ10. Has the contractor instructed all program personnel to become risk identifiers?
- RQ11. Has the contractor developed adequate tools to ensure open, effective two-way communications within its organization and between the prime contractor, subcontractors, and the customer?
- RQ12. Has the contractor discussed the extent that the risk management process is currently in place, in terms of organizations, individuals, and methodology?

- RQ13. Has the contractor discussed his approach to monitoring and statusing the risk handling activities; adding or deleting or adjusting risk areas, or adjusting risk assessments (identification and analysis) as appropriate through out the contract period of performance?

**Obj.2. Define and implement a risk assessment methodology. Perform a thorough cost, schedule, and performance risk assessment and periodic reassessments against identified risk areas.**

- RQ1. Has the contractor developed and documented ground rules and assumptions to be used for risk assessment purposes?
- RQ2. Has the contractor described its risk identification approach for both system-level and lower WBS level risks?
- RQ3. Has the contractor described the risk analysis methodology for cost, performance and schedule risk?
- RQ4. Has the contractor described the methodology in sufficient detail to permit evaluation of its suitability?
- RQ5. Does the contractor's methodology addresses both probability and consequence of occurrence components of risk?
- RQ6. Does the contractor's methodology include the use of ordinal probability and/or consequence of occurrence risk scales? If so, does the contractor perform any mathematical operations on values obtained from these scales (because this will lead to erroneous results)?
- RQ7. Does the contractor's methodology address risk assessment areas associated with C,P,S risk that are likely to exist (e.g., design and engineering, manufacturing, supportability, technology and threat risk)?
- RQ8. Is the contractor's methodology suitable for evaluating each system segment (e.g., space, ground and launch) as required?
- RQ9. Is the contractor's methodology suitable for evaluating hardware, software and integration risk issues?
- RQ10. Has the contractor addressed potential risk assessment areas that may be driven by other "requirements" imposed on the program (e.g., changing environmental regulations, a computer security, or a total system security risk assessment as part of threat risk assessment)?
- RQ11. Has the contractor described the results of the "bottoms-up" C,P,S risk assessment performed against the specific design and technical program management approach selected?
- RQ12. Has the contractor previously used the methodology he proposed to use?
- RQ13. Has the contractor addressed risk assessment areas associated with C,P,S risk that are likely to exist (e.g., design and engineering, manufacturing, support, technology and threat risk)?
- RQ14. Has the contractor evaluated each system segment (e.g., space, ground and launch) as required?
- RQ15. Has the contractor evaluated hardware, software and integration risk issues?
- RQ16. Has the contractor provided and used ground rules and assumptions in the risk assessment?
- RQ17. Has the contractor provided documentation of all items assessed as having medium or high risk, including: (1) a brief technical description of the item, and (2) risk analysis results.
- RQ18. Has the contractor analyzed and provided results for both probability and consequence of occurrence components of risk, plus the time to initial impact?
- RQ19. Has the contractor provided information in sufficient detail that the government evaluator can replicate the results for identified medium and high risk items given the contractor's: (1) risk assessment methodology, (2) ground rules and assumptions and (3) programmatic and technical descriptions of the items?

**Obj.3. Develop a risk handling approach for all items identified as medium or high risk in the risk assessment.**

- RQ1. Has the contractor provided the risk handling approach, including option selected (assumption, avoidance, control or transfer), for all items identified as medium or high risk in the risk assessment?
- RQ2. Does the risk handling approach for each item contain meaningful tasks that can potentially lead to risk reduction (e.g., parallel alternate development/design; rapid prototyping, etc.) rather than simply identifying the problem and collecting information?
- RQ3. Has the contractor provided cost, performance, and schedule impacts associated with risk handling approaches for each identified medium or high risk item?

- RQ4. Has the contractor described and provided the criteria used to exercise each risk handling provision associated with items identified as medium or high risk?
- RQ5. Are risk handling plans integrated across IPTs and up through the IPT structure to ensure that the team works together on them and key milestones can be achieved by the date required?
- RQ6. Is there evidence that the risk management function and program management have evaluated risk handling plans for adequacy and non-conflicting objectives? Have these evaluations included adequacy of the plan, cost effectiveness, schedule effectiveness, resource allocation adequacy and availability, and ensured compatibility between risk handling plans and program objectives?

**Obj.4. Implement and monitor all risk handling activities.**

- RQ1. Has the contractor discussed how risk handling approaches will be implemented and tracked with time throughout the program phase for each medium or high risk item?
- RQ2. Has the contractor provided appropriate cost, performance, and schedule metrics (including earned value measures and TPMs) to be used to track and evaluate the progress in reducing risk for the item?
- RQ3. Has the contractor described how the risk handling process is integrated with the program’s IMS and IMP, including potential risk reduction and key program milestones?
- RQ4. Has the contractor described how it will allocate resources against items identified as having medium or high risk?
- RQ5. Has the contractor assigned an “owner” to each item identified as medium or high risk?
- RQ6. Does a system exist which provides interested program and government personnel access to ongoing risk handling plans, schedules, and status of risk handling activities?
- RQ7. Does a plan for monitoring the effectiveness of the risk handling process exist and will it be (has it been) implemented?
- RQ8. Has the contractor described how risk handling activities are statused across IPTs and up through the IPT structure?
- RQ9. Does the contractor describe how risk analysis levels are adjusted to account for progress in handling where appropriate?
- RQ10. Does the contractor address how risk areas can be added or deleted or adjusted as the program proceeds?

**Obj.5. Establish quantified acceptable risk levels to be achieved prior to transitioning to the next program phase, and define and implement appropriate risk handling efforts.**

- RQ1. Has the contractor described how it will develop and provide quantified acceptable risk levels to be achieved prior to transition to the next acquisition phase?
- RQ2. Are these quantified acceptable risk levels tied to the IMP and IMS?
- RQ3. Has the contractor provided a schedule for developing the quantified acceptable risk levels to be achieved?

### **3.2 Risk Trigger Questions**

The questions contained in Section 3.1 are used to determine if the activities being proposed or being executed by a contractor meet the basic elements of a good risk management process. At a lower level, trigger questions can be used to for several purposes, including: risk identification, independent assessment of the risk management process, preparation for major program review and milestones, etc. The following trigger questions are examples and should not be considered all encompassing. Both the contractor and the government evaluator should add to these based on their own experiences. As addressed earlier, a single risk issue can translate into one or more risk categories (e.g., technology and support) and result in more than one risk impact (cost, performance and schedule). It is important that for each risk, all risk categories and impacts applicable to it be clearly noted so as to ensure that the evaluation and handling processes adequately address the risk from each of these aspects. To avoid redundancy, trigger questions are listed under only one category, although they often fall into more than one type of risk (e.g. many performance risks also lead to cost and schedule risks). Although some trigger questions only apply to some phases of the program they can often provide insight into why risks have developed and can therefore lead to ideas for ways to handle them.

*Some Candidate Cost (Including Budget) Risk Trigger Questions:*

- Is the budget allocated to each PWBS program element and associated IPT adequate to perform the required work?
- Are budgets adequate to handle the level of requirements/objectives changes that are occurring or are likely to occur?
- Has a Service Component Cost Analysis (CCA) or independent cost estimate (ICE) been performed?
- Has a quantitative cost risk analysis been included in the CCA or ICE?
- Have ground rules and assumptions for deriving probability distributions for PWBS elements included in a cost risk analysis been clearly specified?
- Have uncalibrated ordinal scales been erroneously used to generate probability distributions for PWBS elements in a cost risk analysis?
- Are there state-of-the-art PWBS elements that could greatly affect program cost?
- Has the cost of complying with applicable security requirements been included in the budget?
- Has the cost of complying with applicable environmental requirements been included in the budget?
- Are there areas of concern where the potential for delays in development, manufacturing, or demonstration of a product could result in a cascading effect, such as a substantial increase in system cost?

*Some Candidate Schedule Risk Trigger Questions:*

- Is the schedule allocated to each PWBS program element and associated IPT adequate to perform the required work?
- Has an adequate schedule been provided to allow for dependencies between related tasks or disciplines (i.e. if task B cannot be started until task A has completed does task B's schedule start before task A is likely to be done)?
- Is the schedule adequate to handle the level of requirements/objectives changes that are occurring or are likely to occur?
- Does a validated IMS exist?
- Has a quantitative schedule risk analysis been performed on the IMS?
- Has an independent schedule assessment been performed?
- Have ground rules and assumptions for deriving probability distributions for PWBS elements included in a schedule risk analysis been clearly specified?
- Have uncalibrated ordinal scales been erroneously used to generate probability distributions for PWBS elements in a schedule risk analysis?
- Are there state-of-the-art PWBS elements that could greatly affect program schedule?
- Are there any critical lead time concerns?
- Are there technical risks or requirements uncertainty that lie in the schedule critical path?
- Has the time associated with complying with applicable security requirements been included in the schedule?
- Has the time associated with complying with applicable environmental requirements been included in the schedule?
- Are there manufacturing limitations (e.g. test facility backlog, simulation modeling tools availability) which lie in the critical path?

*Some Candidate System Engineering and Technical Risk Trigger Questions:*

- Have requirement(s) been implemented such that a small to medium change in requirements has the potential to cause large cost, performance or schedule system ramifications?
- To what extent can requirements be traded between each other and versus the design's potential C,P,S?
- Are requirements well understood by the government and contractor(s)?
- Are program requirements stable?

- Is there adequate traceability from design decisions back to requirements to ensure that the impact of design changes on requirements can be adequately assessed?
- To what extent is the user assisting in the design trade process?
- Are interfaces clearly defined?
- Do the interfaces have clearly defined ownership to ensure adequate attention to details?
- Is there a clearly defined configuration management plan and is it being followed?
- Is there a clearly defined requirements verification plan and is it being followed?
- Are appropriate lessons learned from prior programs and this program integrated into the design to ensure problems do not recur?
- Are system implications of key design decisions unclear?
- Do design(s) or requirement(s) push the current state-of-the-art?
- Have the designs/concepts/components been proven in one or more existing system (flight if satellite, ground if ground support)?
- Will slightly decreased performance adversely impact the ability to meet system objectives (e.g., are margins adequate)?
- Is there adequate design margin to meet system reliability, maintainability, and supportability requirements?
- Are there state-of-the-art PWBS elements that could greatly affect program performance?
- Is the design easily manufacturable/producible/reworkable/upgradable (i.e. operator independent, correctable if a problem is identified after it has been built, etc.)
- Are design decisions evaluated to ensure life cycle costs are not increased by seemingly simple solutions early in the design development phases (i.e. save now, pay later)?
- Has the system been designed to easily accommodate pre-planned product improvements? (Note to CPAT User: If this is not a contract requirement, then this question could be out of scope. Check with the Government Contracting Officer.)
- Are field or on orbit failures tracked against root causes for adequacy of design, manufacturing, and test of components/subsystems?
- Has the concept for operating/maintaining/decommissioning or disposal of the system been adequately defined to ensure the identification of all requirements?
- Have potential parts obsolescence problems been considered and properly evaluated? Are these risks accounted for in the design phase?

*Some Candidate Support Risk Trigger Questions:*

- Are adequate spares included in the program to support the maintenance concept and operational requirements, including surge?
- Are realistic repair and transportation times included in the sparing/warranty models to achieve adequate operational capability?
- Are the (government or contractor) depots prepared to maintain critical resources (skilled workers, processes, critical materials, data systems, etc.) for the entire time the system may be in use?
- Has the concept for operating/maintaining/decommissioning or disposal of the system been defined to ensure the identification of all requirements?
- Are adequate levels and amounts of technical data generated and delivered to enable support at each of the required support levels in the deployment phase?

*Some Candidate Manufacturing Risk Trigger Questions:*

- Is the design easily manufacturable/producable/reworkable?
- Are there any products where a viable manufacturing process must be developed?
- Have the necessary facilities been identified and availability problems been resolved?
- Have the necessary personnel been identified and availability problems been resolved?
- Have the necessary support equipment (test equipment, computer resources, software, ground stations or terminals, etc.) been identified and availability problems been resolved?
- Is there sufficient test equipment and special tooling to support this and other programs being produced simultaneously in the event that problems cause schedule delays?
- Are training materials/courses available where required?
- Are an adequate number of suppliers available for key components?
- Has the test plan been reduced without supporting data to demonstrate this reduction will not adversely affect the quality of the product(s) produced?
- Do producibility problems exist on related product lines associated with common processes or design rules used for this contract?
- Are there environmental risks associated with the manufacturing or deployment of the system?
- Have environmental impacts been adequately evaluated and planned for?

*Some Candidate Program Management Risk Trigger Questions:*

- Are there any key suppliers whose financial health is in question?
- Are there any suppliers considering or likely to consider discontinuing the item they are providing?
- Are there adequate tools to ensure open, effective two-way communications between the prime, any subcontractors, and the customer?

## Annex 1 Glossary

consequence of occurrence	A measure of the severity of the occurrence of the event (e.g., failure). In effect, this requires the identification of what the consequences are and the degree of their impact. Quantitative consequences (e.g., dollars for cost and time for schedule) are needed to estimate true risk. Ordinal risk scales cannot yield cardinal consequence values unless the scales were originally derived or calibrated from such values (which is almost never the case). Consequently, mathematical operations should never be performed on ordinal risk scales since the values will be meaningless and potentially lead to erroneous risk management results (e.g., incorrect prioritization of risks for risk handling funding allocation).
Cost As an Independent Variable (CAIV)	Addresses methodologies to acquire and operate affordable DoD systems by setting aggressive, but achievable, cost objectives and managing achievement of these objectives. In CAIV, cost objectives should be set to balance mission needs with projected out-year resources, taking into account anticipated process improvements in both DoD and defense industries. In effect, cost is treated as more of an input or independent variable, and less of an output or dependent variable, in the process of acquiring DoD systems.
cost risk	A risk which has the potential to effect the cost of the product(s) to be delivered under the current or future contracts. Focuses on the sufficiency of funds specified for the item for its acquisition. This can range from a single acquisition phase through the complete program life cycle.
exit criteria	Exit criteria serve as gates that, when successfully passed or exited, allow the program to continue with additional activities within an acquisition phase or be considered for continuation into the next acquisition phase. Exit criteria are some level of demonstrated performance (e.g., a level of engine thrust), the accomplishment of some process (e.g., manufacturing yield) or event (e.g., first flight), or some other criterion (e.g., satisfactory risk handling) that indicates that aspect of the program is progressing satisfactorily.
Integrated Master Plan (IMP)	A description, usually contractual, of the applicable documents, significant accomplishments, accomplishment criteria, events, and critical processes necessary to satisfy all contract requirements.
Integrated Master Schedule (IMS)	The schedule showing the time relationship between significant accomplishments, events, and the detailed tasks (or work packages) required to complete the contract. The IMS uses (and extends if necessary) the same indexing (or single numbering system) as used in the Integrated Master Plan (IMP).
Integrated Product Team (IPT)	Team composed of specialists from all applicable functional disciplines working together (1) to deliver products and processes that affordably meet all requirements at acceptable risk and (2) to enable decision makers to make the right decisions at the right time by timely achievement of the significant accomplishments in the Integrated Master Plan (IMP).
manufacturing risk	The ability of the production process to manufacture the required quantities of an item within the technical specifications, given the available resources.
probability of occurrence	The probability that an event will occur. Ordinal risk scales cannot yield probability values unless the scales were originally derived or calibrated from such values (which is almost never the case). Consequently, mathematical operations should never be performed on ordinal risk scales since the values will be meaningless and potentially lead to erroneous risk management results (e.g., incorrect prioritization of risks for risk handling funding allocation).
risk level	The combined effect of the probability of occurrence and a measured or assessed consequence given that occurrence.

risk analysis	Risk analysis is the process of examining each identified program risk and critical technical process risk. It refines the description of the risk, isolates the cause, and determines the impact of the program risk in terms of its probability of occurrences, its consequences, and its relationship to other risk areas or processes.
risk assessment	The process of identifying and analyzing program area and critical technical process risks. It includes risk identification and risk analysis.
risk assessment areas	The program risk areas generally required by DoD 5000.2-R (15 March 1996) are C,P,S risk. A number of additional risk areas have historically been evaluated, however these additional risk areas can be decomposed into C,P,S risk components. Never-the-less, other risk areas that contribute to a program's C,P,S risk may be developed and analyzed as needed (e.g., resource risk, changing threat risk).
risk handling	The process that selects and implements options to get risk to acceptable levels, given program constraints and objectives.
risk handling plan	The plan identifies the steps to be taken, their schedule, responsible parties, success criteria, current status, and impact on the overall risk level from completion of each step.
risk identification	The process of examining each program element and critical technical process to identify risk areas.
risk management	Risk management is the act or practice of controlling risks that have a potential for causing unwanted program impacts. This process includes: planning a structured approach (risk planning), identifying and analyzing risk items and areas (risk assessment), developing risk handling plans, and monitoring risk handling activities to determine how risks have changed (risk monitoring). Risk management process activities are performed in an iterative fashion.
Risk Management Plan (RMP)	The Risk Management Plan describes the program's (contractor and/or government, as appropriate) risk management process, including: risk planning, risk assessment (identification and analysis), risk handling and risk monitoring activities.
risk monitoring	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 or executes risk handling plans, as appropriate.
risk planning	The process of developing and documenting organized, comprehensive and interactive strategy and methods for identifying and tracking risk areas, developing risk handling plans, performing risk assessments to determine how risks have changed, and planning adequate resources.
schedule risk	A risk that could effect the timely completion of a key milestone. Focuses on the adequacy of the time specified for the item for its acquisition.
support risk	The degree to which the system design meets stated quantitative (e.g., mean time between failure) and qualitative peacetime readiness and wartime utilization requirements. This includes the composite of considerations necessary to achieve the effective and economical support of a system for its life cycle, and integrated logistics support resources-related Operations and Support (O&S) cost considerations.
technical risk	A risk associated with meeting a performance requirement, usually associated with pushing the state of the art, meeting weight or speed restrictions, or integrating something complex that has never before been done.
Work Breakdown Structure (WBS)	A product-oriented hierarchical tree composed of the hardware, software, services (including cross-product tasks such as systems engineering), data, and facilities that encompass all work to be carried out under the program or contract along with a dictionary of the entries in the tree. The WBS for the entire program is called the Program or Project WBS (PWBS). The WBS for the work under the contract is called the Contract WBS (CWBS) and is prepared in accordance with the contract.

## Annex 2 Acronyms

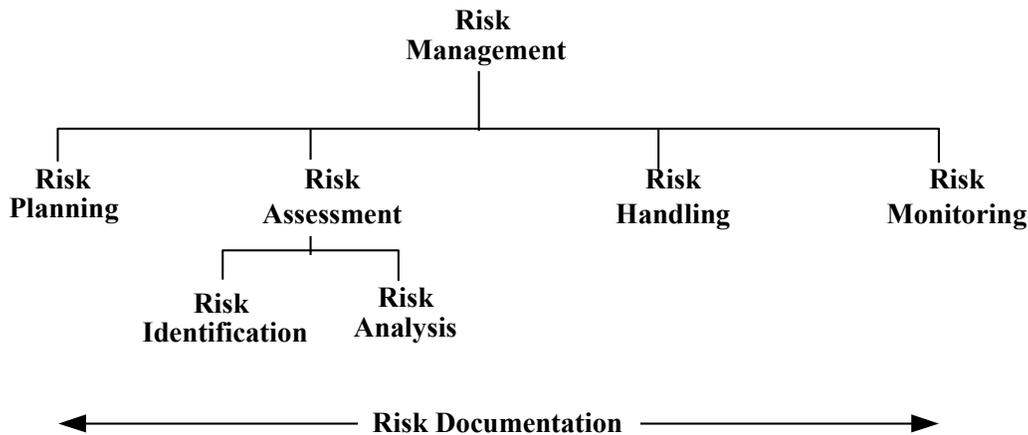
AFAM	Air Force Acquisition Model
AFMC	Air Force Material Command
ASC	Aeronautical System Center
CAIV	Cost as an Independent Variable
CCA	Component Cost Analysis
CDRL	Contract Data Requirements List
CPAT	Critical Process Assessment Tool
C,P,S	Cost, performance and schedule risk areas
CSOW	Contract Statement of Work
CWBS	Contract Work Breakdown Structure
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EMD	Engineering and Manufacturing Development
ICE	Independent Cost Estimate
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IPT	Integrated Product Team
IRMP	Integrated Risk Management Process
LAAFB	Los Angeles Air Force Base
LCC	Life Cycle Cost
MAIS	Major Automated Information Systems
MDAP	Major Defense Acquisition Programs
MNS	Mission Need Statement
ORD	Operational Requirements Document
OSD (A&T)	Office of the Secretary of Defense (Acquisition & Technology)
PPI	Proposal Preparation Instructions
PWBS	Program or Project Work Breakdown Structure
RFP	Request for Proposal
RMP	Risk Management Plan
SEMP	System Engineering Management Plan
SMC	Space & Missile Center
SOO	Statement of Objectives
TPM	Technical Performance Measurement
WBS	Work Breakdown Structure

Note: Terms directly related to risk management are defined in Annex 1.

## Annex 3 Some Aspects of the Risk Management Process

### INTRODUCTION

A simplified risk management process, identical to the OSD risk management process, composed of risk planning, risk assessment (identification and analysis), risk-handling, and risk monitoring functions, is given in Figure 2. The process illustrated in Figure 2 is not the only acceptable risk management process, but representative of a suitable process. For example, the four functions associated with this process may be encompassed by another process implementation using different function names or even a different number of functions. The key consideration is that the underlying material discussed for each function is used to ensure that program risk areas are adequately addressed regardless of the risk management process implemented.



**Risk Management Process Structure**  
**Figure 2**

As discussed in Section 1.1, the risk management process is performed throughout the program life cycle. The process should be executed on a somewhat regular basis, such as a major review conducted once a year with updates quarterly, in addition to material required to support major program milestones and reviews.

In general, risk assessment results should be evaluated by succeeding contractor and government organizational levels where possible to ensure accountability and to identify and eliminate potential inconsistencies, items omitted, and inappropriate risk level assignments. It is important, however, that higher level program management not arbitrarily influence and bias the risk assessment and risk handling results or the resulting value of the risk management process will be substantially degraded.

Medium or high risk areas may reflect missing capabilities in the program's organization or in supporting organizations. They may also reflect technical difficulties in the design or development process. In either case, "management" of risk involves using program management assets to reduce the identified risks. A risk viewed as easily manageable by some managers may be considered hard to manage by less experienced or less knowledgeable managers. Consequently, the terms "high," "medium (or moderate)," or "low" risk are relative terms. In addition, some managers may be risk averse and choose to avoid recognized risk at all reasonable cost. Other managers may be risk seekers and actually prefer to take an approach with more risk. Hence, the terms "high," "medium," and "low" risk may change with the turnover of managers and their superiors as much as with the program events.

Each item for a given risk category that is assessed to have a medium or high risk should be reported with sufficient documentation to permit evaluation by the government program office. This information should include both risk analysis results and a corresponding risk handling plan (including cost, performance, and schedule metrics

for risk monitoring). (Items assessed as low risk for a given risk area should be documented at least once per year by the contractor and the results and associated supporting information furnished to the government.) Each medium or high risk item should be assigned contractor and government IPT “owners” who are responsible for follow-up to ensure adequate risk handling plans are generated, executed and monitored.

A wide variety of organizational implementation strategies can be used for risk management, and it is not the purpose of this CPAT to suggest only one. In effect, risk management process implementation should be adapted to the organizational structure of the program. It is far more important that the four essential aspects of the risk management process (risk planning, assessment (identification and analysis), handling and monitoring) be properly performed within a given program than to rigidly follow a given implementation. In any event, the relevant contractor IPT(s) should be interacting closely with cognizant government IPT(s) throughout the program’s life to reduce potential risk assessment errors and problems with supporting documentation, and to enhance the risk handling process. In fact, it may often be possible (as well as advisable) to include government members on the contractor IPTs in either advisory or direct participant roles to increase the efficiency of the program’s risk management process.

A range of possible risk management process implementations is possible depending upon the program’s organizational structure and desires of senior government and contractor program personnel. Three possible implementations, focused on the risk assessment and risk handling functions, are now briefly discussed which illustrate a variety of different approaches.

The first implementation is applicable to programs having only a single government and single contractor IPT. In this case, the risk management function is embedded into the systems engineering and program management function performed by the single government and contractor IPTs. With this approach the contractor performs a risk assessment, and the government evaluates and updates the results (as warranted) and approves the results. The contractor also develops a risk handling plan, and the government evaluates and updates the plan (as warranted) and approves it. The contractor then implements the resulting approved risk handling plan and monitors progress being made to reduce the level of risk present.

The second implementation is applicable to programs having multiple government and contractor IPTs. In this case, the risk management function can be handled by the government and contractor systems engineering or program management (or equivalent) IPT. It is similar to the first approach except that the focus of responsibilities is on an IPT where risk management is a major responsibility rather than one of many responsibilities.

The third implementation is applicable to programs having multiple government and contractor IPTs plus separate risk management organizations that at a minimum perform the risk assessment and risk handling aspects of this process. How this third implementation is realized depends in part upon the level of insight versus oversight that the government program office possesses for a given program.

In any event, relevant contractor IPTs identify and assess candidate risk items for each identified risk area. The contractor IPTs should then provide results to a central contractor Risk Management Board (RMB) or equivalent, which independently screens and verifies the results, generates an overall ranking of the results (e.g., “top twenty” risk items), and reviews candidate risk handling plans. (Prime contractors are strongly encouraged to utilize expertise from cognizant sub-contractors, particularly when the sub-contractors will supply specific hardware or software deliverables to the program.) The risk assessment results for the contractor’s design; methodology used in assessing the evaluated items; “top twenty” list and “watch list” of key risk items; and risk handling (e.g., control) plans for all items identified as medium or high risk are then provided to the government program office.

In cases where limited government oversight exists, the contractor may receive feedback from the government, adjust risk assessment results and/or risk handling plans as warranted, then implement the risk handling and monitoring functions.

In cases where substantial government oversight exists, the contractor risk assessment and risk handling outputs, along with inputs from government program office IPTs and other assessment teams (e.g., design assessment) and from other government facilities (e.g., laboratories), are forwarded to a working level government

program office Risk Management Advisory Group (RMAG) or equivalent. The RMAG performs a number of candidate functions, including developing, reviewing and revising risk assessments and the risk handling plan. The government program office RMB (or equivalent), composed of senior SPO managers, is responsible for approving and prioritizing risk assessment results provided by the RMAG (e.g., the program office's "top twenty" risk items), finalizing and approving the risk handling plan, and allocating resources in conjunction with the contractor to mitigate risks. (The government RMAG and RMB and contractor RMB are needed in addition to existing IPT(s) to ensure the completeness and accuracy of the risk analysis results and the completeness and suitability of the risk handling plan.)

A key activity of the risk management process is the implementation of the risk handling plan. Each IPT implements portions of the risk handling plan approved by the contractor or government RMB that is assigned to them and ensures prompt notification of both problems identified and resolved as they occur. Risk handling activities are statused across IPTs to the contractor RMB (and government RMAG and RMB or equivalent when substantial government oversight exists). This statusing should include progress, conclusions where they exist, new concerns as a result of risk handling activities, and a reassessment of the risk handling plan for adequacy in content, budget, resources, and schedule. Risk levels should be adjusted to account for progress in risk handling where appropriate. (A comparable risk handling approach should also be developed for the single IPT and multiple IPT cases given above. Again, the important consideration is that the relevant functions are implemented rather than how the implementation actually occurs.)

The risk planning, assessment, handling and monitoring functions are now discussed in more detail. (Note: risk documentation is discussed below in the context of each of the risk management functions and a separate, brief summary discussion on risk documentation is also provided.)

## **RISK MANAGEMENT PROCESS FUNCTIONS**

### **RISK PLANNING**

As with any other activity, risk management must be planned and organized. Although the government program manager is ultimately responsible, neither he/she nor any one individual within the program should be the sole creator or proprietor of program risk management. Risk management requires a team effort that cuts across the government and contractor program offices, and each functional area needs to be involved with specific responsibilities assigned. The use of multidisciplinary teams is an appropriate way to examine risk areas, and is a step toward reducing risk through increased interaction among the functional areas.

Risk planning is the process to force organized purposeful thought to the subject of eliminating, minimizing, or containing the effects of undesirable occurrences. Personnel and other resources both needed to perform and available to perform risk management should be identified. Focal points should be identified by WBS element and corresponding IPT for the generation of risk assessments. Responsibilities and roles should be clearly delineated to ensure that appropriate attention is applied to each risk area, WBS element, and other considerations (e.g., exit criteria, if applicable).

Risk planning consists of the up-front activities needed for a successful risk management program. At the end of one program phase, risk planning is the heart of the preparation for the next program phase.

Suitable risk assessment methodologies (for both the "probability" (likelihood) and consequence of occurrence terms) and techniques, along with ground rules and assumptions for their use, must also be developed and documented. Similarly, suitable risk analysis and risk handling documentation formats should be developed.

The risk management process must be integrated with the program's IMS and IMP and yield outputs suitable for the IPS needed for major program milestones and to support other program activities (e.g., provide a rationale for program budgeting). Risk management milestones, as well as design changes, experiments, technology demonstrations, and process developments that affect the risk management process should also be integrated into the program's IMS and IMP. This should also include inter-relationships between these items to permit identification of potential critical path issues, etc.

## **RISK ASSESSMENT**

Risk assessment is the process of identifying and analyzing program area and critical technical risks. It includes risk identification and risk analysis.

### **RISK IDENTIFICATION**

Risk identification is the process of examining each program area and critical technical item to identify risk areas. Here, it is necessary to identify all potential risk areas. This may include receiving inputs from the government, contractor(s), and users for concerns and problems. The thoroughness with which this identification is accomplished can have a substantial impact on the effectiveness of the risk management process.

Numerous methods exist for identifying risk. Any source of information that allows recognition of a potential problem can be used for risk assessment. These include, but are not limited to:

- Expert interviews
- Analogous systems
- Review of plans
- Systems engineering documentation
- Requirements documents
- Lessons-learned files
- Design and program reviews
- Trade studies/analyses
- Technology assessments
- Results generated from cost and schedule estimating models

Each of these risk identification approaches may prove helpful to a given program. However, using any method in a "cookbook" manner may cause unique risk aspects of the program to be overlooked. The PM should review the strengths and weaknesses of the risk identification approach and insure that other factors that may affect program risk have not been overlooked.

### **RISK ANALYSIS**

Risk analysis is the process of examining each identified program risk and critical technical item risk. It refines the description of the risk, isolates the cause, and determines the impact of the program risk in terms of its probability (or uncertainty) of occurrence, its consequence of occurrence, and its relationship to other risk areas or processes. (While the time to the risk impacting the program is not a true component of risk, it is nevertheless a metric that should be computed and reported if possible.) The purpose of risk analysis is to discover the cause, effects, and magnitude of the perceived risk, and to identify and evaluate alternative options.

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 likelihood (probability) and consequences have been quantified using compatible cardinal scales. In such a case, mathematical manipulation of the values may be meaningful and provide some quantitative basis for the ranking of risks. In many cases, however, risk scales are actually ordinal scales, reflecting only relative standing between scale levels and not actual numerical differences. Any mathematical operations performed on ordinal scales, or a combination of ordinal and cardinal scales, can provide information that will at best be misleading, if not completely meaningless, possibly resulting in erroneous risk ratings. Hence, mathematical operations should never be performed on scores derived from raw (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.)

When performing a risk analysis, an objective evaluation should be made to prevent intentionally or unintentionally biasing the results. The risk analysis results and subsequent risk handling plans should be objective and unbiased to the extent possible. It is particularly important that this occur when data is being prepared for the government and contractor program managers to prevent unhealthy distortions in the program's risk management process.

A variety of tools should be considered for use in performing the program risk analysis. The selected tools may vary with risk area, amount and type of available inputs, and program maturity. Typical tools for use in risk analysis include, but are not limited to:

- Schedule network models, such as Program Evaluation Review Technique (PERT)
- LCC models (which may include WBS simulations)
- Quick Reaction Rate/Quantity Cost Impact Models
- Decision Analysis (e.g., trade-off analysis and utility analysis)
- Ordinal risk scales

Several products should be an output of the risk analysis. The exact names and format of these products is not important versus their content. For example, summary charts should be prepared for all items with a medium or high risk rating for each risk area. These include a concise summary of each risk item (which contains an item description, risk source, potential program impact, and handling strategy), and risk analysis data sheet (which contains risk (uncertainty) and consequence of occurrence values for each risk area and the rationale for assigning each value).

Another highly desirable risk analysis product is a risk priority matrix, which is illustrated in Figure 3. Here, a simple two-dimensional plot of uncertainty and consequence or occurrence levels is constructed for all items evaluated in the risk analysis. (More granular risk analysis results can be reduced to low, medium and high categories. It is not recommended that low, medium and high risk analysis levels be used directly, as they are generally too coarse to accurately describe the uncertainty or consequence of occurrence present.) From Figure 3, the risk associated with a given analyzed item will fall into one of the 3x3 cells--items having higher risk tend to be towards the upper right hand portion of the matrix, while lower risk items tend to fall towards the lower left hand portion of the matrix. The numbers placed in the cells correspond to priorities for risk reduction, and the results should be carried over to the risk handling function for the development and implementation of risk handling activities. Figure 3 contains five levels of priority, which can readily be reduced to three levels of priority if necessary (cells with scores of 1 or 2 become high, cells with scores of 3 become medium and cells with scores of 4 or 5 become low). Although this representation is somewhat simplistic, it does provide the risk management team with a logical method to recognize medium and high risk items and it addresses both the uncertainty and consequence of occurrence terms of risk (rather than simply one or the other).

Other highly desirable risk analysis output include a "top twenty" (or similar) risk item list and a "watch list".

A "top twenty" (or similar) risk item list is helpful for risk tracking purposes. It should contain the risk score, risk area, and rationale that led to the item receiving the prioritized risk ranking. Another useful list is one containing all items assessed as high risk, along with the risk score, risk area, and supporting rationale. Similarly, a list can be generated containing all items assessed as medium risk. The value of such lists is that they provide a simple summary of the key program risks, and reduce the chance that an important risk issue will not be considered.

**Risk Priority**

“Probability”	H	3 H,L	2 H,M	1 H,H
	M	4 M,L	3 M,M	2 M,H
	L	5 L,L	4 L,M	3 L,H
		L	M	H

**Consequence**

**Risk Priority Matrix  
Figure 3**

A "watch list" includes the identification of consequences that are likely to occur for a given problem and the indicators of the start of the problem. An example of this is the cost risk of production due to an immature technical data package. A typical watch list is structured to show the trigger event or item (for example, long lead items delayed), the related area of impact (production schedule) and later, as they are developed, the risk handling actions taken to avoid/minimize the potential for or impact from that event (such as ensuring early identification of long lead items or placing contractor emphasis on early delivery). The watch list is periodically reevaluated and items are added, modified, or deleted as appropriate. Should the trigger events on the watch list occur during a program, there would be immediate cause for impact assessments to be updated and risk handling methods to be selected.

**RISK HANDLING**

After the program's risks have been assessed, the PM must develop approaches to handle those that are significant by analyzing various risk handling techniques and selecting those best fitted to the program's circumstances. These approaches should be reflected in the program'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.

There are essentially four risk handling techniques:

- (1) risk assumption, which 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
- (2) risk avoidance, which eliminates the sources of high risk and replaces them with a lower-risk solution
- (3) risk control, which manages the risk in a manner that reduces the likelihood of its occurrence and/or minimizes the risk's effect on the program, and
- (4) risk transfer, which is the reallocation of risk from one part of the system to another, or the reallocation of risks between the prime contractor and subcontractors or between the government and the prime contractor

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

- 1) For each identified risk, all potentially applicable techniques should be identified and evaluated, using the following criteria:
  - a) Feasibility of the technique—This addresses the ability to implement the technique and includes an evaluation of the potential impact of the technique in the following areas:
  - b) Technical considerations, such as testing, manufacturing, and maintainability, caused by design changes resulting from risk handling techniques.
  - c) Adequacy of budget and schedule flexibility to apply the technique.
  - d) Operational issues such as usability (man-machine interfaces), transportability, and mobility.
  - e) Organizational and resource considerations, e.g., manpower, training and structure.
  - f) External considerations beyond the immediate scope of the program, such as the impact on other complementary systems or organizations.
- 2) Expected effectiveness of each technique in controlling program risk—risk assessment techniques, along with other techniques such as trade studies and sensitivity analyses, can be useful in determining this expected effectiveness.
- 3) Cost and schedule implications of the technique—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. The approval and funding of risk handling techniques should be part of the trade-off process that establishes and refines the CAIV cost and performance goals.
- 4) 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, an attempt should be made to identify any additional parameters that may become critical to technical performance as a result of implementing them.

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

Unfortunately some programs fall into the trap of thinking that simply going to meetings, making phone calls or even “worrying” about a problem will be sufficient to effectively handle risk. In reality, risk handling is a proactive discipline that does not happen on its own. In addition, it must be enmeshed with the program’s IMS and IPS so that key schedule milestones both exist and are monitored with regards to progress made to date in mitigating risk. While unanticipated, fortunate development outcomes sometimes occur, program’s must generally devise and implement viable handling activities by fixed, known schedule milestones to have a realistic chance of reducing potentially adverse C,P,S and risk impacts on the program.

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

## **Risk Assumption**

This technique is used in every program, and acknowledges the fact that, in any program, risks exist that will have to be accepted without any special effort to control them. Such risks may be either inherent in the program 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 the development; this monitoring should be well-planned from the beginning.

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, re-testing, requirements review, etc.

Ensure that the necessary administrative actions are taken to quickly implement these management actions, such as contracts for industry expert consultants, arrangements for test facilities, etc.

Whenever a risk is assumed, a schedule and cost reserve should be set aside to cover the specific actions to be taken if the risk occurs. If this is not possible, the program may proceed within the funds and schedule allotted to the effort. If the program 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.

## **Risk Avoidance**

This technique reduces risk through the modification or elimination of those operational requirements that cause the risks. It requires close coordination with the users. Since this technique results in the reduction of risk, it should generally be considered initially 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.

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 contractor, government program office and the user with an understanding of what the real needs are and allows them to establish accurate system requirements. 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 the requirements specified in terms of functions and capabilities, rather than a 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.

## **Risk Control**

In this risk handling technique, active steps are taken to reduce the likelihood of a risk occurring and to reduce the potential impact on the program. All risk control steps share two features: they require a commitment of program resources, and they may require additional time to accomplish. Thus, the selection of risk control actions will undoubtedly require some tradeoff between resources and the expected benefit of the actions.

Risk control involves the development of a risk reduction plan, with risk reduction 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 the risk monitoring section. Some of the many risk control actions include:

**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 a system that meets the same performance requirements.

**Backup Choices Available.** Sometimes, a design option may include several risky approaches, of which one or more must come to fruition to successfully meet system requirements. However, sometimes 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 contractor, government program office and the user is necessary to implement lower capability options.

**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 requirements. 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.

## **Risk Transfer**

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 one party and another.

In the reallocation of risk method, design requirements that are risk drivers are reallocated to other system elements, which may result in lower system risk

Risk transfer has two distinct dimensions. First is the reallocation of risk during the concept development and design processes from one part of the system to another such that the overall system risk is reduced but ideally system requirements will still be met. For example, for a complex software development effort the risk may possibly be reduced by transferring a function from a selected software module to a hardware module. 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.

The second dimension of risk transfer involves a reallocation of risks between the government and the prime contractor or between contractors (on a team). This reallocation is done on the basis that the receiving activity (e.g., prime contractor) is better suited to manage the risk and will aggressively do so via the identification, evaluation, selection and implementation of the most appropriate risk handling option. The most common application of this option is the transferring of risk from the program office to the prime contractor. This is done through the contracting process and takes the form of contract type, performance incentives, warranties, etc. This can also be applied between the prime contractor and subcontracts, subcontractors and vendors, etc. Risk transfer is a form of risk sharing and not risk abrogation on the part of the program manager.

For the risk transfer approach to be effective, the risks transferred from one party to another must be those that he has the capacity to control and best manage. These are generally risks associated with technologies and processes used in the program—those for which he can implement proactive solutions. A number of options are

available to implement risk transfer from one party to another: warranties, cost incentives, product performance incentives, and various types of cost-based contracts.

## **RISK MONITORING**

Risk monitoring is a process that systematically tracks and evaluates the performance of risk handling actions against established metrics throughout the acquisition process. It should also include the results of the periodic reassessments of program risk to evaluate both known risks and any new risks to the program. As the program progresses, the monitoring process will identify the need for additional risk handling options.

An effective risk monitoring effort can provide information to show if risk handling actions are not working and which risks are on their way to becoming actual problems. The information should be available in sufficient time to take corrective action. The functioning of IPTs is crucial to effective risk monitoring. They are the “front line” for obtaining indications that risk 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. Specific indicators to be monitored and information to be collected, compiled, and reported early in the planning phase of the process. Normally, documentation and reporting procedures are developed as part of risk management planning before contract award and should use, as much as possible, the contractor’s reporting system.

To ensure that significant risks are effectively monitored, risk 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 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 should be documented both formally and informally. 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 be dependent on the program.

Many techniques and tools are available for monitoring the effectiveness of risk handling actions, and the best suited ones should be selected. 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 risk handling activities by comparing the 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.

The indicators/metrics selected to monitor program status should 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 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.

## **Risk Documentation**

Successful risk management programs include timely specific reporting procedures tied to better communication. Normally, documentation and reporting procedures are defined as part of the risk management strategy planning before contract award, but they may be added or modified during contract execution as long as the efforts remain within the scope of the contract or are approved as part of a contract change. Some teams use risk management notebooks with team subsections kept up-to-date; scheduled feedback of risk information to team leaders and program management; and communication with the customer on risks when appropriate.

The need for good documentation is well recognized but is lacking in product. Some important reasons for having sound risk management documentation include:

- It tends to insure a more comprehensive risk assessment than using less formal documentation.
- It provides the rationale for why program decisions were made, and can potentially assist junior engineers through the program manager.
- It provides a good baseline for program assessments and updates as the program progresses.
- It can assist in tracking the progress of supporting technology programs versus a baseline.
- It provides a management tool for use during the execution of the program, including permitting a more objective assessment of how additional funds or potential budget cuts should be allocated.
- It provides program background material for new personnel.