Administrative Change to AFMCPAM 63-101, Life Cycle Risk Management

OPR: HQ AFMC/ENS

Cover statement, "COMPLIANCE WITH THIS PUBLICATION IS MANDATORY" should be deleted.

(Pamphlets are not mandatory per Table 2.1, item 12, page 35 of AFI 33-360. Nondirective publications are informational and suggest guidance that you can modify to fit the circumstances. Complying with publications in this category is expected, but not mandatory.)

4 APRIL 2012

BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE MATERIEL COMMAND
PAMPHLET 63-101

27 APRIL 2011

Acquisition

LIFE CYCLE RISK MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFMC/ENS

Certified by: HQ AFMC/ENS (Daniel Goddard)

Supersedes: AFMCPAM 63-101, 9 JULY 1997

Pages: 74

This pamphlet does not apply to the Air National Guard (ANG). This pamphlet does not apply to US Air Force Reserve (USAFR) units. This pamphlet is intended to provide program managers and their program management team a basic understanding of the terms, definitions and processes associated with effective risk management.

The risk management concepts and ideas presented in this pamphlet are focused on encouraging the use of risk-based management practices and suggesting ways to address the program risk without prescribing the use of specific methods or tools. This pamphlet was prepared as a guide, with the expectation that program risk management processes will be developed to meet the intent of this document. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims**/.

SUMMARY OF CHANGES

This document has been substantially rewritten and must be completely reviewed.

Chapter 1—INTRODUCTION **4**

1.1. Pamphlet Roadmap. 4

1.2. Overview. 4

1.3. Purpose. 4

1.4. Risk Management: 5

Figure 1.1. AF Life Cycle Risk Management Process (ref. AFPAM 63-128, Chapt 12). 7

1.5. Life Cycle Risk Management Participants: 7

1.6. Effective Risk Management Characteristics and Guidelines. 7

Chapter 2—NEW PROGRAM RISK MANAGEMENT **9**

2.1. Overview: 9

2.2. Initial Program Planning: 9

2.3. Early Industry Involvement. 10

2.4. Using Risk Assessments to Support Program Planning: 11

Table 2.1. Early Risk Assessment Example. 12

2.5. Source Selection Acquisitions 12

2.6. Sole Source Acquisitions: 15

Table 2.2. Sole Source Risk Assessment Example. 15

2.7. Contingency Plans: 16

Table 2.3. Monte Carlo Simulation Contingency Cost Estimate Input Example. 17

Figure 2.1. Monte Carlo Simulation Contingency Cost Estimate Output Example. 17

2.8. Risk Monitoring. 18

2.9. Risk Management Indicators. 19

2.10. Program Management Indicator System. 19

Table 2.4. Indicators Data. 19

2.11. Supporting Tools. 20

Table 2.5. Watchlist Example. 20

2.12. Management Actions. 21

2.13. Risk Management Board. 21

Chapter 3—EFFECTIVE RISK ASSESSMENTS **23**

3.1. Overview. 23

Table 3.1. Example of Successful Program Management of ESOH Risks. 28

3.2. Summary. 29

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 31

Attachment 2—RISK MANAGEMENT PLAN (RMP) FORMAT 36

Attachment 3—SAMPLE RISK MANAGEMENT PLAN 41

Chapter 1

INTRODUCTION

1.1. Pamphlet Roadmap. This risk management pamphlet applies to acquisition risks and is organized into three general segments. **Chapter 1** provides an executive-level overview of risk management. **Chapter 2** provides high level concepts related to application of risk management on new programs. **Chapter 3** focuses on integrating risk assessments into program management. **Attachment 2** contains a risk management plan template, while **Attachment 3** contains a sample risk management plan geared towards major programs, but tailorable to smaller programs.

1.2. Overview. Risk management is an integral part of the overall acquisition process. When a disciplined, comprehensive risk management program is implemented throughout a program's life cycle, critical program risks are properly identified and suitable handling plans are developed and implemented. A well-executed life cycle risk management process is essential for balancing cost, schedule, and performance goals, especially on programs with designs that approach or exceed the state-of-the-art.

1.2.1. Risk management is not a separate program function but an integral part of the overall program planning and management process. In order to be effective, the risk management process must be recognized as part of everyone's job and a central program management activity, and not something limited to the program manager or chief engineer. Any program element associated with cost, schedule, and performance has a direct interface with the risk management process.

1.2.2. It is important to remember that risk management is employed throughout the program's life cycle. A risk management strategy should be developed early in the program (as early as the Analysis of Alternatives (AoA) Study Plan) and addressed continually throughout the program through final disposition. This process does not change fundamentally as the program progresses, although refinement will occur as program unknowns become knowns and its design matures.

1.2.3. It is essential that programs define and implement appropriate risk management and contingency plans. Risk management should be designed to enhance program management effectiveness and provide program managers a key tool to reduce life cycle costs.

1.2.4. An effective life cycle risk management process requires a commitment on the part of the program manager and the program office to be successful. Many impediments exist to risk management implementation. One good example is the natural reluctance to identify real program risks early for fear of jeopardizing the program's support or even continuation. Another example is the lack of sufficient funds to properly implement the risk handling process. However, when properly implemented, the risk management program supports setting realistic cost, schedule, and performance objectives and identifies areas that require special attention.

1.2.5. Planning a good risk management program integral to the management process ensures that risks are handled at the appropriate management level.

1.3. Purpose. This pamphlet:

1.3.1. Provides guidance to help establish a Life Cycle Risk Management framework for risk management planning, risk identification, risk analysis, risk handling/mitigation planning, risk mitigation implementation and tracking for all acquisition programs.

1.3.2. Serves as a source of general guidance which can be tailored to fit within the program and statutory requirements.

1.3.3. Includes discretionary acquisition guidance and information, expert wisdom, best practices and lessons learned.

1.3.4. Applies to all elements of a program (system, subsystem, hardware, software, and acquisition/sustainment supply chains).

1.3.5. Should be used in conjunction with related directives, instructions, policy memoranda, or regulations issued to implement the mandatory procedures contained in DoD and AF directives and instructions.

1.3.6. Can be tailored into a single management process to provide an efficient, integrated acquisition process supporting the orderly flow of program decisions, milestones, and other essential activities.

1.3.7. Discusses performance within the context of the following areas of technical risks: threat; requirements; technology; engineering; manufacturing; environmental, safety, and health; logistics and supportability; test and evaluation; operational support; demilitarization and disposal.

1.3.7.1. This pamphlet uses the term “acquisition” generically to apply to all programs, regardless of life-cycle phase—from laboratory research programs to major weapon or information system development programs—through sustainment and disposal.

1.4. Risk Management:

1.4.1. Risk. Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan, external data providers, etc.) as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS). Risk has three components:

1.4.1.1. A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring.

1.4.1.2. A probability (or likelihood) assessed at the present time of that future root cause occurring.

1.4.1.3. The consequence (or effect) of that future occurrence.

1.4.1.3.1. Failure to account for the severity of the consequences means that risks may be misstated. For example, if a particular event has a high probability of failure (PF), but only a small impact, then it is unrealistic to call it a high risk. On the other hand, a number of risks can have a low probability of occurrence but have consequences so serious that they are treated as moderate risks. A classic case is safety issues, which typically have been handled as moderate or high risks, despite their relatively low probability of occurrence.

1.4.2. Risk Management Process. Risk management is the act or practice of controlling risk. This process includes identifying and tracking risk areas, developing risk mitigation plans as part of risk handling, monitoring risks and performing risk assessments to determine how risks have changed. Risk management process activities fall into the following five broad elements and are performed with many iterative feedback loops.

1.4.2.1. *Risk planning* consists of the up-front activities necessary to execute a successful risk management program. It is an integral part of normal program planning and management. The planning should address each of the other risk management functions, resulting in an organized and thorough approach to assess, handle, and monitor risks. It should assign responsibilities for specific risk management actions and establish risk reporting and documentation requirements. Risk planning should also include development of training materials and the conduct of training to program personnel. Program managers are required to prepare and maintain Risk Management Plans per AFI 63-101. A sample format and Risk Management Plan template can be found in **Attachment 2** and **3** of this pamphlet.

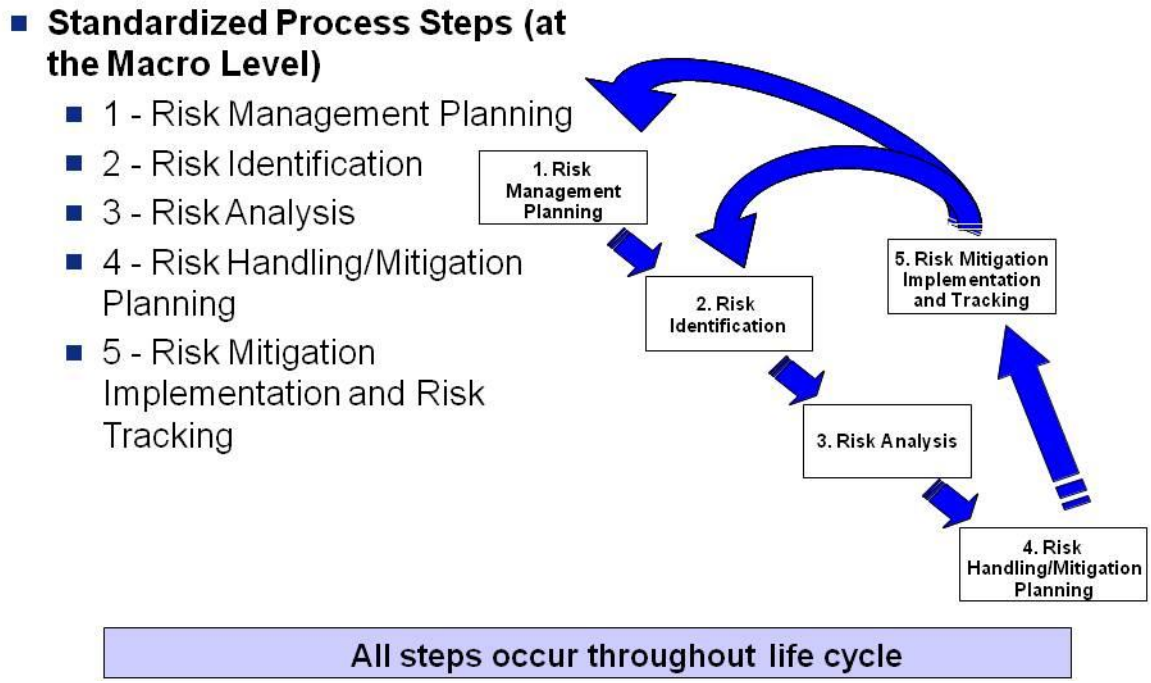
1.4.2.2. *Risk identification* is the process of examining the program and each critical process to identify and document risk areas. Risk identification begins as early as possible in successful programs and continues throughout the program with regular review and analysis.

1.4.2.3. *Risk analysis* is the process of examining each identified program and process risk, isolating the cause, and determining the impact. Risk impact is defined in terms of its probability of occurrences, its consequences, and its relationship to other risk areas or processes. Consequences are typically identified and analyzed in terms of performance, schedule, and cost.

1.4.2.4. *Risk handling/mitigation planning* is the process that identifies, evaluates, selects and implements options in order to set risk at acceptable levels given program constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, and the cost and schedule impact. The most appropriate strategy is selected from these handling options and documented in a risk handling plan. There are a number of techniques or options for handling risks: avoidance, control, transfer, monitor, research, and assumption.

1.4.2.5. The intent of *risk mitigation implementation and tracking* is to ensure successful risk mitigation or acceptable handling occurs. Risk implementation directs the teams to execute the defined and approved risk mitigation plans; and outlines the risk reporting requirements for on-going monitoring. Effective risk tracking helps to identify what planning, budget, and requirements and contractual changes may be needed; provides a coordination vehicle with management and other stakeholders, and documents the change history. Risk tracking systematically tracks and evaluates the performance of risk handling actions against established metrics throughout the acquisition process

Figure 1.1. AF Life Cycle Risk Management Process (ref. AFPAM 63-128, Chapt 12).



1.5. Life Cycle Risk Management Participants:

1.5.1. Involve Everyone In Risk Management. Effective risk management requires early and continual involvement of all of the program team as well as outside help from subject-matter experts, as appropriate. Participants include the customer, laboratories, acquisition, contract management, test, logistics, and sustainment communities; and industry.

1.5.2. Develop Close Partnership With Industry. Effective management of a program's risk requires a close partnership between the government, industry, and later, the selected contractor(s). The program manager should understand the differences in the government's view of risk versus industry's view and ensure all risk management approaches are consistent with program objectives. Both the government and industry need to understand their respective roles and authority while developing and executing the risk management effort.

1.6. Effective Risk Management Characteristics and Guidelines. Acquisition programs run the gamut from simple, straightforward procurements of mature technologies which cost a few thousand dollars to state-of-the-art and beyond programs valued in the multibillions of dollars. Effective risk management programs generally follow consistent characteristics and guidelines across all programs despite these vast differences in program size and technologies.

1.6.1. Characteristics of Successful Risk Management. Successful programs will have the following risk management characteristics:

1.6.1.1. Feasible, stable, well-defined, and well-understood user requirements.

1.6.1.2. A close partnership with user, industry, and other appropriate participants.

1.6.1.3. A planned risk management process integral to the acquisition process, which should include management buy-in, an open environment, and integration with program management.

1.6.1.4. A program assessment performed early to help define a program which satisfies the user's needs within acceptable risk.

1.6.1.5. Identification of risk areas, risk analysis and development of risk handling strategies.

1.6.1.6. Acquisition strategy consistent with risk level and risk handling strategies.

1.6.1.7. Continuous reassessment of program and associated risks.

1.6.1.8. A defined set of success criteria that covers all performance, schedule, and cost elements.

1.6.1.9. Metrics used to monitor effectiveness of risk handling strategies.

1.6.1.10. Formally documented. ***NOTE:*** Air Force programs identified on the Acquisition Program Master List or Sustainment Program Master List, designated product groups, and other specified systems are required to use the Probability of Program Success (PoPS) tool to assess and document risk objectively and consistently per AFI 63-101.

1.6.2. Successful risk management programs will incorporate the following guidelines:

1.6.2.1. Assess program risks and develop strategies to manage these risks during each phase.

1.6.2.1.1. Identify early and intensively manage those design parameters which critically affect capability, readiness, design cost, or life cycle costs.

1.6.2.1.2. Use technology demonstrations/modeling/simulation and aggressive prototyping to reduce risks.

1.6.2.1.3. Include test and evaluation as part of the risk management process.

1.6.2.2. Include industry participation in risk management. Offerors must identify risks and develop plans to manage those risks as part of their proposals.

1.6.2.3. Use proactive, structured risk assessment and analysis process to identify and analyze risks.

1.6.2.3.1. Identify, assess and track technical performance, schedule, and cost risk areas.

1.6.2.3.2. Establish risk mitigation plans.

1.6.2.3.3. Provide for periodic risk assessments throughout each program phase.

1.6.2.4. Establish a series of "risk assessment events," where the effectiveness of risk reduction conducted to date is reviewed. These events are to be tied to the integrated master plan (IMP) at each level and have clearly defined entry and exit criteria.

1.6.2.5. Include processes as part of risk assessment. This would include the contractor's managerial, development, and manufacturing processes.

1.6.2.6. Use AF standard evaluation criteria defined in AFI 63-101 and AFPAM 63-128 for assigning risk ratings (low, moderate, high) for identified risk areas.

Chapter 2

NEW PROGRAM RISK MANAGEMENT

2.1. Overview:

2.1.1. Administration of a successful program requires effective risk identification, assessment, and management. Each program, to be most effective, should implement risk management processes from the Acquisition Planning Period through program execution.

2.1.2. The program manager should structure the program plan, develop the acquisition strategy, generate Request for Proposal (RFP), write the source selection plan, evaluate the proposals, and select the contractor team with program risk as a key consideration. This should be done within an integrated management framework that allows the government to manage program and associated top-level risks while the contractor is responsible for management of product and process risks, and maintenance of accountability in design.

2.1.3. This chapter will briefly discuss initial program planning activities, and then describe how risk management processes can be used through the program acquisition process to promote program success.

2.2. Initial Program Planning:

2.2.1. Acquisition program planning should take place within an integrated management framework which follows the generation of the initial capabilities document (ICD), capability development document (CDD), capability production document (CPD), Life Cycle Management Plan (LCMP) technical performance requirements, work breakdown structure (WBS), Integrated Master Plan (IMP), Integrated Master Schedule (IMS), Life Cycle Costs (LCC), and program budget.

2.2.1.1. The program office team must understand the operational capabilities required. This would apply to either a new system or a modification to an existing system.

2.2.1.2. The program office team then must define the technical performance requirements based on inputs from both industry and government technical stakeholders. Once this is done, a program that fulfills those requirements can be developed.

2.2.1.3. When the conceptual program has been developed, an initial WBS can be defined with all follow-on program documents tied to the WBS.

2.2.1.4. A planning program IMP should be developed, using as much industry input as practical, to define the program critical events with the appropriate success or exit criteria to satisfy those events.

2.2.1.5. After the planning IMP is developed, an IMS can be generated to provide the schedule details. This IMS is based on the IMP events and expands them to the activity level for the entire program. The IMS should include all programmatic activities included in the IMP. The program office team should identify required activities and tasks, and develop a program schedule. These activities must be detailed sufficiently by knowledgeable and experienced people, so that critical and high-risk efforts are identified as realistically as possible even though it is very early in the program's life cycle.

2.2.1.6. When the preceding activities are complete, an LCC estimate can be developed to support the initial budget submissions. Both the schedule and cost estimates developed by the team should address the uncertainty caused by the risks identified. The budget submission should represent the program office's best assessment of an executable program.

2.2.2. The activities listed above should be accomplished as early as feasible, and updated as the program progresses. Risk assessments should be performed to provide the necessary insight needed to support these program planning activities.

2.3. Early Industry Involvement. Since the program's actual risk is greatly affected by the capability of the government and contractor team to develop and manufacture the system, early involvement with industry is critical to program planning. Industry's developmental and manufacturing processes and tools, the availability of resources including skilled personnel, and the previous experience of the government and contractor team all influence their ability to handle the proposed system development and subsequent production. Therefore, an effective risk management process includes market research and an evaluation of the capabilities of potential sources, and getting industry involvement in program planning as early as feasible.

2.3.1. Industry Day. A powerful tool for determining general industry capabilities to support identification of potential program risk is to conduct an Industry Day. To avoid potential problems in the competitive process and ensure a "level playing field" is maintained, an announcement in *FedBizOpps* should be made to inform all potential future offerors that the government may conduct an Industry Day and request responses from all interested parties who may wish to take part.

2.3.1.1. The basic steps in the process are:

2.3.1.1.1. Establish the criteria for the capability review,

2.3.1.1.2. Identify the potential companies who will participate in the review,

2.3.1.1.3. Identify the potential companies not able to attend Industry Day, but still wish to participate in the review,

2.3.1.1.4. Provide an advance copy of the review material to those contractors,

2.3.1.1.5. Select the review team, ensuring it has the necessary mix of technical and acquisition talents,

2.3.1.1.6. Provide training to the team on the purpose of the review and on how to achieve a common understanding of the review criteria,

2.3.1.1.7. Conduct the review and evaluate the results,

2.3.1.1.8. Provide feedback to each company on the results of their review and assessment,

2.3.1.1.9. Provide the results to the program office.

2.3.1.2. Defense Contract Management Agency (DCMA) can be a valuable source of information for industry performance and capabilities. In addition, the Industrial Analysis Center within DCMA can perform capability assessments on both industry and industry sectors.

2.3.2. Determining Risk Sharing. One of the key elements of the acquisition strategy is to determine whether a particular risk is to be shared with the contractor or retained exclusively by the government. For example, by directing the use of government-furnished equipment (GFE), the government usually retains the entire risk related to the inherent performance of the GFE. However, a less clear case would be an example derived from the definition of a system's operational environment. If a system's vibration environment is unknown, this could potentially affect the system's performance - including reliability - and should be considered a program risk area.

2.3.2.1. At least two choices are possible for sharing this risk:

2.3.2.1.1. The government makes an engineering estimate of the expected range of vibration environments, and provides a requirement to the contractor that the system meet those environments. In this case, the government retains the risk; if the environment is worse than specified, the contractor has no responsibility to fix the system (as long as it met the specification). Or,

2.3.2.1.2. The government includes a contract work task to measure the range of environments and to design the system to survive those environments. In this case, the contractor has a responsibility to make the system perform in its operational environment.

2.3.2.2. The key concept here is that the government SHARES the risk with the contractor, not TRANSFERS risk. The program office always has a responsibility to the system user to develop a capable system, and can never absolve itself of that responsibility. Therefore, all program risks, whether primarily managed by the program office or by the developing contractor, are of interest to the program office and must be assessed and managed by the program office. Once the program office has determined which risks and how much of each risk to share with the contractor, it must assess the total risk assumed by the developing contractor (including subcontractors).

2.3.2.3. A prime program consideration is the equitable allocation of program risk, with its associated cost consequences, between the government and its contractors. Contractors should not be required to accept financial risks which are inconsistent with their ability to control and absorb these risks. These financial risks are largely driven by the underlying technical and programmatic risks inherent in a program. This requires the government contracting officer to select the proper type of contract based on an appropriate risk assessment, in addition to the selection principles set forth in Part 16 of the “Federal Acquisition Regulation.” In short, there must be a clear relationship between the selected contract type and the assessed program risk.

2.4. Using Risk Assessments to Support Program Planning:

2.4.1. Systems engineering analysis and risk assessments provide additional information to the program planning team during the program planning. This information allows program managers to make tradeoff decisions between alternative acquisition and technical strategies, balancing technical performance, schedule and cost program objectives.

2.4.2. After the program's risks have been identified and assessed, the approach to handling each moderate to high risk must be developed. The various risk handling options are

analyzed and those best fitted to the program's circumstances selected. These are included in the program's acquisition strategy.

2.4.3. The actual example found in **Table 2.1** is provided to depict how the risk assessment process can be tailored to be an invaluable planning tool in the early stages of a program.

Table 2.1. Early Risk Assessment Example.

Objective	Perform an initial iteration of the risk assessment process to define an executable program and establish a baseline for a Risk Management Plan	
Program Status	The system to be acquired was a state-of-the-art avionics system, which was just entering the flight test phase for the system. The program office was conducting a technology insertion program to reduce risk to the next phase	
Methodology	Developed an initial baseline, networked schedule	
	Divided program activity into five broad areas; Requirements Allocation, Hardware Development, Software Development, System Integration, and System Test	
	Examined areas for major program risks and uncertainties which could affect cost and schedule	
	Performed schedule analysis on major areas of program risk and uncertainty	
	Examined possible effects of schedule deviations on critical paths and program cost	
Risks Identified	Requirements Allocation	Determined to be low risk, so no further cost or schedule analysis was performed
	Hardware Development	Assessed as having internal schedule impacts, but would not affect the program's critical path
		Two Line Replacement Units (LRU) costs would likely increase up to 25-50 percent
		Overall cost increase would likely be $8 million
	Software Development	Best case: 20 percent fewer lines of code, reduced schedule 3 months, save $45 million
		Worst case: 30 percent more lines of code, increased schedule 3 months, cost increase of $68 million
	Systems Integration	This was assessed as reasonable, no cost or schedule excursions
	System Test (only issues found in durability life testing)	Best case: No schedule impact, cost decrease of $3 million
		Worst case: Slip from 16 to 24 months, third item delivery extended 6 months, costs increase $7 million

2.4.4. As can be seen from the example, a risk assessment can be used to identify and quantify the key risk areas in a program. Based on this type of analysis, the program office can modify the program as required to incorporate the selected risk handling approaches into the acquisition strategy.

2.5. Source Selection Acquisitions

2.5.1. Request For Proposal (RFP):

2.5.1.1. The RFP should focus primarily on what is essential for the risk-based source selection decision. Each program will have unique requirements and risks. The RFP should therefore be tailored to reflect the individual needs and risks of that specific program. When tailoring the RFP, use discriminators" that will influence the source selection decision. "Discriminators" are the significant aspects of a program that are expected to distinguish one proposal from another, thus having an impact on the ultimate selection decision. By using these discriminators, the source selection team can provide the SSA with an evaluation that distinguishes among competing proposals in those areas the government believes are most important. This facilitates selecting the offeror(s) most likely to deliver the best value to the government and to perform the resulting contract(s) successfully. (ref. AFFARS MP5315.3)

2.5.1.2. The source selection team, in consultation with other stakeholders, shall determine the extent of risk analysis necessary to support the acquisition. It is prudent to perform some form of risk assessment for all competitive acquisitions in order to identify high-risk areas, to determine discriminators for source selections, and to identify incentive focus areas. It's these discriminators that should be used to establish the evaluation subfactors. After the government's initial look, it is important to obtain industry input on the risk assessment results. (ref. AFFARS MP5315.3)

2.5.1.3. Based on the results of the analysis, a revised IMP and IMS, and an updated LCC estimate can be prepared. The quality of this risk assessment will be significantly improved by as much interaction with industry as possible. The technical performance, schedule and cost issues identified should be discussed in the presolicitation conference(s) before the draft RFP is released. In this way, the critical risks inherent in the program can be identified and addressed in the RFP.

2.5.1.4. In the solicitation, offerors should be asked to develop a contract IMP and an IMS for inclusion in their proposals to reflect how they propose to do the work. All risks should be clearly linked to the requirement. It is paramount that the RFP stipulate offerors address the risks and proffer mitigation strategies in their proposals. This risk analysis should identify the expected risk areas and the offeror's recommended approaches to minimize the effects of those risk areas. This will support the government's source selection evaluation and the formulation of a most probable cost estimate for each proposal.

2.5.2. The Offeror's Proposal:

2.5.2.1. The offeror's program plan must be developed and documented in the proposal at an adequate level to also identify risks in the offeror's approach and define risk management activities to be employed throughout the program. The program plan should provide a WBS, a top-down list of activities and critical tasks starting with the IMP, associated schedules of tasks and milestones rolled up into the IMS, and an estimate of the funds required to execute the program, with a particular focus on the resource requirements for the high-risk areas.

2.5.2.2. The information required and the level of detail will depend on the acquisition phase, the category and criticality of the program, as well as the contract type and dollar

value. However, the detail submitted with the proposal must be at the level necessary to identify possible conflicts in the schedule and support the government's proposal evaluation. The information required to be submitted after contract award should be at the proper level to support the decision process during program execution.

2.5.3. Risk-Based Source Selection:

2.5.3.1. Assessing Proposal and Contractor Performance Risks. The purpose of a source selection is to select the proposal that represents the best value. To perform this evaluation, the government must assess both proposal risk and performance risk for each proposal. Risk assessment in the source selection MUST be done entirely within the boundaries of the source selection process. Prior assessments of any of the offerors may not be applicable or, if applicable, must be considered and used under very specific procedures set forth in the source selection plan.

2.5.3.1.1. *Proposal risk* refers to the risk associated with the offeror's proposed approach to meet the government requirements. The evaluation of proposal risk includes an assessment of proposed time and resources, and recommended adjustments.

2.5.3.1.2. Past Performance Evaluation. The past performance evaluation results in an assessment of the government's confidence in the offeror's ability to fulfill the solicitation requirements while meeting schedule, budget, and performance quality constraints. The past performance evaluation considers each offeror's demonstrated record of performance in supplying products and services that meet users' needs. The performance confidence rating is normally assessed at an overall factor level. (ref AFFARS MP6315.3). Proposal risk and performance confidence will be discussed in the ensuing sections.

2.5.3.2. Proposal Risk Assessment. The source selection evaluation team must evaluate the risks inherent in each offeror's proposal. This analysis of proposal risk should be performed according to the risk definitions and evaluation standards developed for the source selection.

2.5.3.2.1. The technical and schedule assessments are primary inputs to the cost estimate for each proposal. It is important that the evaluation team estimate the additional resources needed to overcome risk for any factors with "moderate" or "high" risk ratings. These resource requirements may be defined in terms of additional time, manpower loading, hardware, or special actions such as additional tests. However, whatever the type of the resources required, it is essential that the cost estimates derived be fully integrated and consistent with the technical and schedule evaluations, and that the results reflect the time and resources required to execute the program.

2.5.3.3. Performance Confidence Assessment. This is an evaluation of the likelihood (or government's confidence) that the offeror will successfully complete the solicitation's requirements; the evaluation is based upon past performance. The assessment of the principal offeror should take into account the past and present performance of critical subcontractors, who will perform major or critical aspects of the requirement. Performance confidence is normally assessed by the Performance Confidence

Assessment Group, a group of experienced government personnel appointed by the source selection advisory council Chairperson. Performance confidence may be separately assessed for each evaluation factor or may be assessed for the offeror as a whole. The performance confidence assessment may be provided directly to the source selection advisory council/authority for final decision or indirectly through the Source Selection Evaluation Board. The assessment relies heavily, but not exclusively, on the contractor performance evaluations and surveys submitted by program offices and DCMA.

2.6. Sole Source Acquisitions:

2.6.1. In sole source situations, the risk assessment can be developed with close contractor participation, although the level of participation will depend on the situation and the status of the sole source approval. To be of greatest benefit, the program office team should perform a risk assessment before the Justification and Authorization (J&A) is completed and RFP is released to the contractor. As noted previously, DCMA may be able to provide key support for this effort. After receipt of the contractor's proposal, a second risk assessment based on the proposal can be an invaluable aid to contract negotiations and program planning.

2.6.2. Before RFP release, a systematic risk assessment is accomplished; the IMP and IMS are updated; the LCC is revised; and a track to any previous risk assessment is prepared. Once this has been completed, the formal RFP should be prepared with this updated information and sent to the contractor.

2.6.3. The RFP may ask the contractor to propose an IMS that has resource loading for the high-risk activities which had been identified. This resource detail should support the contractor's proposal and show the government evaluators that the risk mitigation activities have been planned and included in the price. This will also help the government understand the full scope of the effort. However, whatever the proposal data requirements are, a risk assessment should be performed on the proposal, and the analysis should become a critical ingredient in the fact-finding process and a key input to the negotiation objective.

2.6.4. After the contract has been negotiated, the program IMP, the contract IMP and IMS, and the LCC estimate should be updated. A track should also be documented from the previous risk assessment. This documentation will serve as an invaluable record for program managers and decision-makers during program execution. The updated LCC may serve as the basis for the next budget submission. **Table 2.2** contains an example of a risk assessment performed on an acquisition program in a sole source environment.

Table 2.2. Sole Source Risk Assessment Example.

Objective	Conducted pre-RFP and proposal receipt risk assessments
Methodologies	Composed team of technical experts
	Software Development Risk Assessment - used parametric models, including PRICE-S, REVIC (Revised Enhanced Intermediate Version of COCOMO), COCOMO (Constructive Cost Model), SEER (System Evaluation and Estimation of Resources), and SASET (Software Architecture Sizing and Estimating Tool)

	Schedule Risk Assessment - Microsoft Project and CORAM (Consolidated Risk Assessment Methodology)
	Sensitivity Analysis - probabilistic modeling
Scope	Software Development and Integration, Hardware Development, Flight Test Schedules and Support, Schedule Relationships and Durations
Risks Identified	Simulation Software Schedule – High risk
	Operational Flight Test Software – Moderate risk
	Programmatic Impacts – Significant increase in schedule that impacts other tasks
Mitigation Plan	Early testing of software
	Lower percentage of software retest
	Eliminate low priority software changes
	Management indicators in place to check mitigation
	Verify contractor has implemented risk reduction efforts

2.7. Contingency Plans:

2.7.1. Often times risk mitigation efforts do not fully bring the risk to an acceptable level. In many cases, risk mitigation efforts are not possible (i.e. when risks are accepted). For these types of risks, especially those of high concern, contingency plans should be developed that describe the plan that will be implemented if these risk events occur. Contingency funds and schedule are set aside to handle these known risk events. Contingency planning is understandably integral to the program's overall life cycle management plan and other functional plans, such as the systems engineering plan that addresses technical risks.

2.7.2. One of the primary purposes of developing contingency plans is to formally identify contingencies instead of adding generic "padding" to cost and schedule estimates for individual programs. When contingencies are hidden in cost and schedule estimates, the cost and schedule for these programs tend to gravitate toward the estimates whether or not the contingencies are necessary. The formality of contingency planning provides visibility and control to those activities.

2.7.3. Since contingency plans are only implemented in the event that mitigation strategies fail, only a portion of these plans will ever be enacted. Given this situation, it is not necessary to develop cost and schedule reserves for every contingency plan. A Monte Carlo simulation technique that takes into account the probability of occurrence of the risk after mitigation plans have been implemented can be used to develop both cost and schedule reserves for contingency. Further details on Monte Carlo analysis can be found in courses in statistics, financial risk analysis, and also in software tool guides, such as Excel 2007 and Active Risk Manager.

2.7.4. Example of Monte Carlo simulation technique:

2.7.4.1. Contingency reserves are based on confidence levels derived from the Monte Carlo simulation. An 80% confidence interval is recommended as the level to select for cost and schedule reserves. However, the data from the simulation should be analyzed before such a decision is made. Depending on the data, another confidence interval may be more appropriate. The cost reserve is added to the overall budget of the program and the schedule reserve is added to the project reserve schedule.

2.7.4.2. **Table 2.3** illustrates the input used to calculate the confidence interval cost reserve.

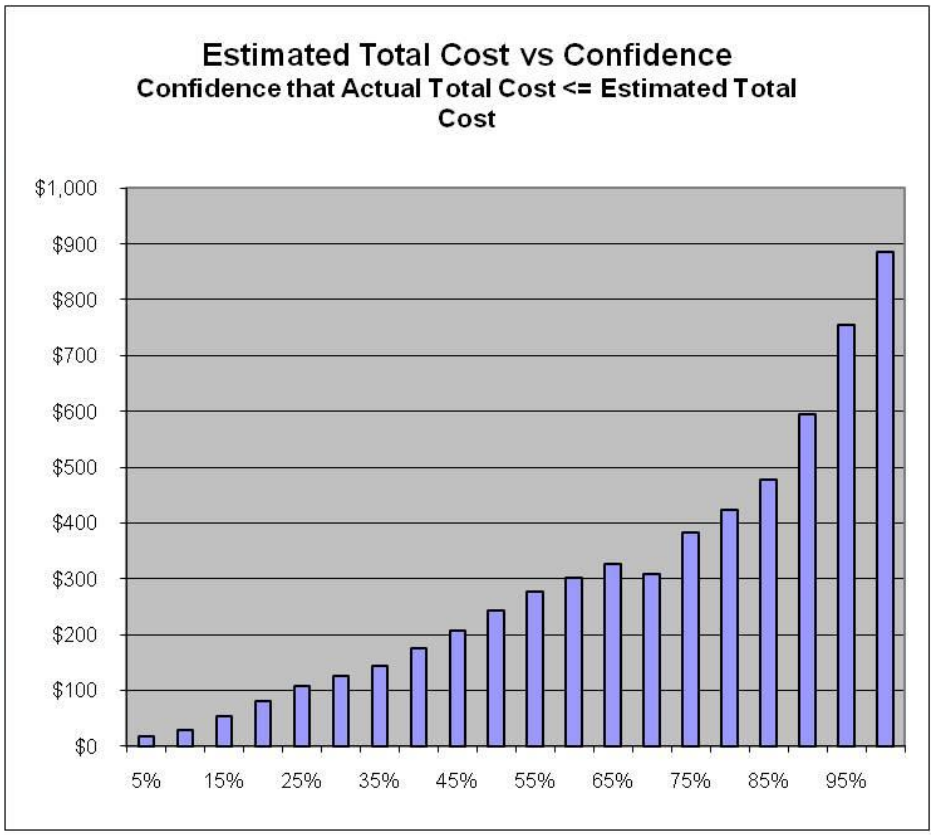
Table 2.3. Monte Carlo Simulation Contingency Cost Estimate Input Example.

INPUTS ($K)			
TASK	EST COST_50	EST COST_90	EST PROB
1	$ 102	$ 133	50%
2	$ 15	$ 20	70%
3	$ 37	$ 48	10%
4	$ 237	$ 308	50%
5	$ 53	$ 53	20%
6	$ 453	$ 453	15%
7	$ 10	$ 20	12%
8	$ 13	$ 13	75%
9	$ 5	$ 5	10%
10	$ 3	$ 3	5%

2.7.4.3. **Figure 2.1** illustrates the output of the Monte Carlo Simulation used to calculate the 80% confidence interval for the contingency cost reserve.

Figure 2.1. Monte Carlo Simulation Contingency Cost Estimate Output Example.

OUTPUTS ($K)	
CONF	TOTAL COST
5%	$ 18
10%	$ 29
15%	$ 53
20%	$ 82
25%	$ 107
30%	$ 126
35%	$ 144
40%	$ 175
45%	$ 206
50%	$ 244
55%	$ 278
60%	$ 302
65%	$ 326
70%	$ 309
75%	$ 382
80%	$ 423
85%	$ 478
90%	$ 594
95%	$ 756
99%	$ 886



2.7.4.4. The schedule reserve is calculated in a similar manner using task times instead of cost estimates for each task.

2.7.4.5. The contingency cost reserve is added as part of the time-phased budget to ensure dollars are allocated in the correct fiscal year in case they are needed. Budget is allocated based on when risk events are likely to occur. The dollar level allocated is based on contingency plan dollar levels and PM judgment. It is important to note the contingency cost reserve is less than the sum total of the costs of all contingency plans; therefore judgment must be used when allocating the cost reserve in the time phased budget. Contingency work packages will only be distributed when the risk event occurs. Contingency plans should be developed for each work package of the project. In addition, "contingency triggers" must be identified for all risks that have contingency plans associated with them. "Contingency triggers" are events, circumstances, or criteria that are defined that serve as a signal for the project manager to implement the contingency plan. These signals are activated when the risk event occurs or when its occurrence is inevitable.

2.7.4.6. For example, a contingency plan for unsuccessful tests due to an immature system under test could be to re-fly these tests once the system under test is fixed. The "trigger" for the event could be the results of data analysis from the previous flight. When the results of flight test data analysis indicate problems that require extra flights, the extra flights (the contingency plan) are placed in the project schedule as tasks. When executed, these tasks will consume some of the schedule reserve laid into the project schedule.

2.8. Risk Monitoring. Once the contract has been awarded (or organic development efforts begun), the risk management process shifts to managing the effectiveness of the selected risk handling approaches. During this process, a number of decisions need to be made. Unexpected difficulties will occur, regardless of the comprehensiveness of the up-front risk assessment. Therefore, the risk management system must be prepared to identify those difficulties when they occur, assess the consequences of those difficulties, and devise effective corrective measures. Even though risk monitoring takes place after contract award, this process should be an integral part of Initial Program Planning.

2.8.1. At this point, tools such as the IMP and IMS can become invaluable program baseline and risk management documents. Because the same or a traceable numbering system was used in the WBS, the contract statement of work and the IMP, a consistent thread links all the items in various program documents. Also, resources can be referenced to the IMS, reporting formats derived from it, and the program office team staffing based on it. When dynamic changes occur in the program, this link will enable the impact of the change to be captured in all program documentation much more easily than it has in the past.

2.8.2. In addition, the program office should include risk assessment and handling activities as key contractual tasks during all acquisition phases to support risk monitoring activities. The contractor(s) must be encouraged to identify program risks and to identify and execute effective handling approaches for each. In conducting these assessments, the contractor(s) should examine the risks to a lower level of detail than the government's assessment. This allows the contractor(s) to identify additional risk areas and promotes better insight into follow-on efforts. The program office should also encourage the prime contractor to

establish risk management requirements for its subcontractors and critical vendors. Results of those efforts should be reported during program reviews.

2.9. Risk Management Indicators. The key to risk management is a good management indicator system that covers the entire program. Clear management indicators should be designed into the risk tracking plan to provide early warning when problems arise and may utilize DCMA inputs. As indications of problems or potential problems are raised, management actions to mitigate those problems should be taken. This indicator system provides feedback to program management on the effectiveness of planned actions, and for the need to readjust the program based on design realities. Triggers, as discussed in paragraph 2.7.4.5., are a type of indicator to execute a specific contingency plan when a predicted risk becomes reality.

2.9.1. In addition to an indicator system, the program office should perform periodic reassessments of program risks. The assessment evaluates both the previously identified risks and examines the program for risks not previously identified. The program office should be re-examining the risk handling approaches concurrent with the risk assessment. As the program progresses, additional risk handling options may surface which should be considered for inclusion in the program.

2.10. Program Management Indicator System. The program management indicator system is the consolidated repository for categories of data received by the program office. The indicators consist of technical performance measures, program metrics, cost performance data, and schedule tracking data.

2.10.1. Technical Performance Measures (TPM). To be effective, TPMs should be established on key program technical characteristics (as defined in the system specifications). They can provide an effective mechanism to monitor the values of the parameters. When TPMs are applied to areas of known risks, they can be used to assess the effectiveness of the various program risk reduction actions. A planned performance profile with warning and action thresholds is normally established for each TPM.

2.10.2. Program Metrics. These are formal, periodic performance assessments of the various development processes, used to evaluate how well the system development process is achieving its objectives. For each program, certain processes are critical to the achievement of program objectives. Failure of these processes to achieve their requirements is symptomatic of significant problems. Metrics data can be used to diagnose and aid in the resolution of these problems. Where TPMs are derived from specification requirements, metrics are derived from programmatic requirements. Program metrics are established and used in a manner similar to TPMs.

2.10.3. Cost and Schedule Performance. The information provided in cost/schedule control system criteria reports provide valuable data which depict how well the program is progressing toward completion. Careful analysis of these status reports can uncover problem areas not previously flagged by the program team.

2.10.4. Examples of the kinds of data for each category are shown in **Table 2.4**.

Table 2.4. Indicators Data.

TECHNICAL PERFORMANCE MEASURES AND PROGRAM METRICS

Key Design Parameters Weight Size Endurance Range Design Maturity Drawing Release Design to Cost Failure Activity	Manufacturing Yields Incoming Material Yields Delinquent Requisitions Unit Production Cost Process Proofing	System Reliability System Maintainability Logistics Related Deliverables Manpower Estimates

COST	SCHEDULE
Cost Performance Index Schedule Performance Index Estimate at Completion Management Reserve	Design Schedule Performance Manufacturing Schedule Performance Test Schedule Performance

2.11. Supporting Tools. In addition to the indicators listed above, there are at least two supporting tools which help in risk management. These tools must be created as part of the Initial Program Planning activities. They are demonstration events and watchlists.

2.11.1. Demonstration Events. For many risks, demonstration events will be defined to assess what risks remain in the development effort. If the event is successful, then the risk has been abated to some degree. If it fails, then the program must either invoke a backup or take additional time and resources to correct the deficiency. Demonstration events are at the heart of the performance requirement and verification, and the IMP/IMS concepts. These demonstration events are laid out as part of the program planning during the risk handling stage of the risk management process. Monitoring the satisfactory completion of these events gives the program a buildup of confidence that program risks are being reduced. Early failures provide warning that a problem exists; if the events are properly planned, they give the program a margin of time to recover from the failures.

2.11.2. Watchlists. This is a listing of critical areas that management will pay special attention to during the execution of the program. The watchlist is developed as a product of the risk assessment, and can vary in complexity. It is normally a simple list of the identified potential risks (see **Table 2.5**). Items on the watchlist should be reviewed during the various program reviews/meetings, both formal and informal. Items can be added to or deleted from the watchlist as the program unfolds.

Table 2.5. Watchlist Example.

MAJESTIC PROGRAM WATCHLIST (Integrating an electronic warfare suite onto an aircraft system) (Program Pre-EMD)	
RISK AREA	DRIVERS
Threat changes	Capability of DRFM (digital radio frequency memory) threat system (ext. IOC 2011). Also, threat signal density based on Defense Intelligence Agency System Threat Assessment Report.

Jammer/aircraft avionics electromagnetic compatibility	Jammer and system radar operate in the same band.
Software algorithms	Correlation between radar warning receiver, integrated reprogramming data and missile warning system. Also, timing requirements between warning and jammer and chaff/flare dispenser.
Cooling for Electronic Warfare suite	Current system marginal. Actual available cooling flow and system duty cycles not firmly established.
Man-machine interface	Electronic Warfare suite integrated information display to operator.
Availability of JP8 system	JP8 bio-fuel system currently in development; initial availability mid-2012.
High velocity maintenance capability of depots	Availability forecast less than requirement; affects maintenance and training requirements.
Producibility of solid state amplifiers	New manufacturing process required to achieve power density requirements.
System integration	Planned suite never installed on large aircraft system.

2.12. Management Actions. Management indicators and supporting tools provide the information necessary to manage the program. Unfavorable trends and incidents must be analyzed and their significance to the program assessed. For those problem areas judged significant to the program, appropriate management actions must be taken. These can either involve the reallocation of resources (personnel, funds and schedule), activation of a contingency plan (such as a backup approach or on-call use of an expert). Severe cases may require readjustment of the program.

2.12.1. It is important that management emphasizes the need to reassess the identified program risks continually. As the system design matures, more information becomes available to assess the degree of risk inherent in the effort. If the risk changes significantly, the risk handling approaches should be adjusted accordingly. If the risks are found to be lower than previously assessed, specific risk handling actions may be reduced or canceled and the funds reprogrammed for other uses. If they are higher or new risks are found, the appropriate risk handling efforts should be put into place.

2.12.2. In addition to reassessing risks, the program office should look for new risk handling options. Different technologies may mature, new products become available in the market places, or information found in unexpected places. All of these may be of use to the program office. A periodic review of new developments in the laboratories and time spent examining what is coming on the market are useful actions for any program.

2.12.3. The program office should assess the risk associated with providing intelligence to the proposed program throughout the lifecycle of the system. This includes the ability to collect, process, analyze, and disseminate the information at the proper fidelity, quantities, and timelines required to meet program needs. The intelligence risk assessment should include the possible impacts on the program and options for mitigating the risks (ref. CJCSI 3312.01A, Joint Military Intelligence Requirements Certification and AFI 63-101).

2.13. Risk Management Board. A risk management tool used on some programs is the risk management board. This board is chartered as the senior program group that evaluates all

program risks, unfavorable event indications, and planned risk abatements. In concept, it acts similar to a configuration control board. It is an advisory board to the program director, and provides a forum for all affected parties to discuss their issues.

2.13.1. Risk management boards can be structured in a variety of ways, but share the following characteristics:

2.13.1.1. They should be formally chartered and have a defined area of responsibility and authority. Note that risk management boards may be organized by the local acquisition center of excellence (ACE) as program office only, program office with other government offices (such as user, DCMA, test organizations), or as combined government-contractor. The structure should be adapted to each program office's needs.

2.13.1.2. Working relationships between the board and the program office staff functional support team should be defined.

2.13.1.3. The process flow for the risk management board should be defined.

2.13.1.4. Boards should have formally-defined interfaces with other program office management elements (such as the various working groups and the configuration control board).

2.13.2. On programs with many moderate to high risk areas, the risk management board provides a sound vehicle to ensure each risk area is properly and completely addressed during the program life cycle. It is important to remember that successful risk monitoring is dependent on the emphasis it receives during the planning process. Further, successful program execution requires the continual monitoring of the effectiveness of the risk handling plans.

Chapter 3

EFFECTIVE RISK ASSESSMENTS

3.1. Overview. **Chapter 1** broadly defined the five basic elements of the life cycle risk management process: *Risk Planning, Risk Identification*, *Risk Analysis, Risk Handling/ Mitigation Planning*, and *Risk Mitigation Implementation and Tracking.* These five elements are often integrated and performed using many feedback loops. **Chapter 2** summarized risk management for new programs. This chapter will describe in more depth the key events, actions, and tasks associated with risk assessments (identification + analysis) and will provide general guidelines on timetables for implementation.

3.1.1. Integrating technical performance, schedule, and cost assessments into a single process provides a final product which starts with well-defined requirements, builds upon a solid technical foundation, develops a realistic program schedule, and documents the resources needed in the program cost estimates.

3.1.2. Risk assessments should be performed to support program definition, planning and key events, which can include acquisition strategy development, RFP preparation, source selection, sole source proposal evaluation, or program reviews and milestone decisions.

3.1.2.1. Risk assessment during source selection is a self-contained process and should not be part of the prior program risk assessment process. The risk assessment should be appropriately marked if restricted access is needed (e.g. For Official Use Only / Source Selection Sensitive / STINFO & Export Controlled / Proprietary / Negotiation Sensitive).

3.1.3. The program or contract-level risk assessment integrates the technical program assessment, schedule assessment, and cost estimate steps using established risk evaluation techniques. A risk assessment should be done periodically throughout each acquisition phase at both program and supplier level.

3.1.4. When the situation demands, a specific team may also perform a risk assessment focused on a lower-level product or specific task. Examples include: 1) projected test cost trades given decreased number of test units, 2) contract production costs for a particular number of units, or 3) independent cost assessment.

3.1.5. Focus Areas. The risk assessment must integrate the technical performance, schedule and cost aspects of the program under review. Each of these focus areas has activities of primary responsibility, but is provided inputs and support from the other two focus areas. This helps to keep the process integrated and to ensure the consistency of the final product. The activities are often tailored, but the typical responsibilities on a risk assessment include:

3.1.5.1. Technical Performance Assessment:

3.1.5.1.1. Provides technical foundation.

3.1.5.1.2. Identifies and describes program risks.

3.1.5.1.3. Prioritizes risks with relative or quantified weight for program impact.

3.1.5.1.4. Analyzes risks and relates them to other internal and external risks.

3.1.5.1.5. Quantifies associated program activities with both time duration and resources.

3.1.5.1.6. Uses risk handling to set risk at acceptable levels given program constraints.

3.1.5.1.7. Scopes schedule and cost consequences if risk mitigation fails.

3.1.5.1.8. Quantifies inputs for probabilistic schedule assessment and cost estimate if this method is used for schedule assessment and cost estimating.

3.1.5.1.9. Documents technical basis and risk definition for the risk assessment.

3.1.5.2. Schedule Assessment:

3.1.5.2.1. Evaluates baseline schedule inputs.

3.1.5.2.2. Incorporates technical assessment inputs to program schedule model.

3.1.5.2.3. Evaluates risk impacts to program schedule based on technical team assessment.

3.1.5.2.4. Performs schedule analysis on program Integrated Master Schedule (IMS).

3.1.5.2.5. Quantifies schedule excursions which reflect schedule impacts if risk mitigation fails.

3.1.5.2.6. Provides schedule impacts for risk handling options as part of risk handling.

3.1.5.2.7. Quantifies schedule excursions which reflect impacts of cost risks, including resource constraints.

3.1.5.2.8. Provides government schedule assessment for cost analysis and year planning.

3.1.5.2.9. Reflects technical foundation, activity definition and inputs from technical and cost areas.

3.1.5.2.10. Documents schedule basis and risk impacts for the risk assessment.

3.1.5.3. Cost Estimate:

3.1.5.3.1. Builds on technical and schedule assessment results.

3.1.5.3.2. Translates technical and schedule risks into “dollars and cents”.

3.1.5.3.3. Provides cost estimates for risk handling options.

3.1.5.3.4. Derives cost estimate integrating technical assessment and schedule risk impacts to resources.

3.1.5.3.5. Establishes budgetary requirements consistent with fiscal year planning.

3.1.5.3.6. Provides program cost excursions from:

3.1.5.3.6.1. Near-term budget execution impacts.

3.1.5.3.6.2. External budget changes and constraints.

3.1.5.3.6.3. Documents cost basis and risk impacts.

3.1.5.4. Risk assessment activities combine the above and:

3.1.5.4.1. After contract award, use risk monitoring to track actual program indicators against baseline performance, schedule, and cost plans as part of continuous program assessments.

3.1.5.4.2. Repeat the above three assessments when technical performance, schedule, or cost metrics indicate changes are significant enough to warrant updating the risk assessment, or when needed to support program decision process.

3.1.5.4.3. Tie technical performance, schedule, and cost focus areas together in feedback loops as needed during initial or periodic risk assessment.

3.1.5.4.4. Document the integrated results of the risk assessment.

3.1.5.5. The scope of each of these focus areas depends on the program and the objective of the risk assessment.

3.1.6. When to Perform Risk Assessments. Risk assessments should be applied early and continuously in the acquisition process, from the time performance requirements are developed. The early identification and assessment of critical risks allows for the formulation of risk handling approaches and the streamlining of both the program definition and the RFP processes around those critical product and process risks. Risk assessments should be used for all major contractual actions and milestone decisions. The following general descriptions will help interpret the risk assessment process:

3.1.6.1. All risk management actions begin with the identification and analysis of the program's risks. The caliber and quality of this effort establishes the effectiveness of the risk management effort. A determination of what the system must do is the necessary starting point for risk assessment. The program requirements need to be established before risks can be identified and their significance analyzed.

3.1.6.2. The level of detail needed is dependent upon the program phase and the nature of the need to be addressed. However, there must be enough detail to allow a general scoping of the level of effort required, technological capabilities needed, and system complexity.

3.1.6.3. Five basic activities should be performed to assess a program's risks effectively:

3.1.6.3.1. First, the program office should establish the basic approach it will use to assess the risks. A comprehensive and consistent approach is needed to ensure all aspects of the program are examined for risk. This should include, but is not limited to, establishing likelihood, cost, schedule, and performance thresholds appropriate to the program.

3.1.6.3.2. Second, the program office should establish the working structure for the risk assessment, and appoint experienced government and industry personnel, as appropriate. This may include the makeup of a risk management board, review frequency, and local review processes.

3.1.6.3.3. Third, identify the risks in the program. The program manager should ensure each program area is examined to identify the risks inherent in that area.

3.1.6.3.4. Fourth, each identified risk needs to be analyzed to determine the consequences of each risk, the significance of those consequences to the program, and the likelihood of the risk actually occurring. Risk analysis is the detailed evaluation of each identified risk area. This analysis examines each risk, isolates the cause and determines the impact of the risk area on the program.

3.1.6.3.5. Fifth, the results of the risk assessment (and associated risk mitigation planning) should be formally documented. This documentation is important because:

3.1.6.3.5.1. Formal documentation tends to ensure a more comprehensive risk assessment.

3.1.6.3.5.2. It provides the rationale for why program decisions were made.

3.1.6.3.5.3. It provides program background material for new personnel.

3.1.6.3.5.4. It provides a good baseline for program assessments and updates as the program progresses.

3.1.6.3.5.5. It provides a management tool for use during the execution of the program. A listing of the expected program risk areas (sometimes called a watchlist) prompts management on areas to monitor.

3.1.6.4. Risk assessment is not a stand-alone program office task. It is supported by a number of other program office tasks. In turn, the results of the risk assessment are used to finalize those tasks. Important tasks which must be integrated as part of the risk assessment process include the requirements analysis/functional analysis (systems engineering), schedule development, and cost estimating.

3.1.7. Early Risk Assessments. A risk assessment which identifies technical performance risks and reflects the resultant program uncertainty in the program planning may suffice for programs in the initial planning and budgeting stages. Because detailed historical data is not always available, program office teams must be resourceful in gathering the judgments of experts to support the risk assessment.

3.1.8. Using Program Risk Level to Streamline Source Selection. The content of the RFP requirements determines how the source selection will be conducted. Therefore, a risk assessment must be performed prior to release of the draft RFP if it is going to influence what information is actually needed in the proposals. To be effective, the risk assessment should be a key element of the acquisition strategy process and source selection plan development. Specifically, the risk assessment should identify those areas which must be included in the RFP to ensure appropriate consideration is given in the source selection evaluation process. These are areas that may very likely affect the source selection decision. Alternatively, the risk assessment can identify areas where risk is very low, and therefore evaluation of the area is NOT needed during source selection. Excluding very low risk areas from source selection can save the offeror time and resources in not having to prepare proposal information, and save the government time and resources in not having to evaluate information that will not affect the source selection decision.

3.1.8.1. The risk assessment process is iterative. Feedback from market surveys and industry comments during presolicitation conferences and draft RFP issuance provide

avenues to identify and define those critical risks to be addressed through the pre-award process.

3.1.9. Risk Assessment Approaches. For each risk assessment, the program office team must establish how the actual assessment will be conducted.

3.1.9.1. At least four choices are available:

3.1.9.1.1. Conduct the assessment as part of the normal activity of the program office.

3.1.9.1.2. Establish a program office risk assessment team, as either a temporary ad-hoc team or a permanent organization.

3.1.9.1.3. Establish a government/industry team.

3.1.9.1.4. Request an outside team or combined program office/outside team assessment. An independent team is not usually in the management chain or directly involved in performing the tasks being assessed. The technique can be used at different program levels, e.g., Program Office, Service Field Activities, Contractors, etc. For Acquisition Category (ACAT) I programs, independent reviews, such as the Air Force Program Support Review, are required prior to major milestone decisions.

3.1.9.2. Each approach has its own merits and costs. However, the choices are not mutually exclusive. Program offices could use two or more of these options in combination or for different aspects of the program. An internal effort should always be conducted so that program office personnel are familiar with the risks. Special teams may be appropriate if the resources needed to do the assessment are beyond those available to the program team.

3.1.9.3. Regardless of the method(s) chosen, the contractor team's input should be solicited and included in the final assessment. If the program is not already on contract, the risk assessment team should also try to gain insight from industry, within the bounds of competitive nondisclosure and protection of proprietary data.

3.1.9.4. Getting a team organized and trained to follow a disciplined, repeatable process for conducting a risk assessment is important, since periodic assessments are needed to support major program decisions during the program life cycle. Experienced teams do not necessarily have to be extensively trained each time an assessment is performed, but a quick review of lessons learned from earlier assessments combined with abbreviated versions of these suggested steps can avoid false starts. Teams should review ground rules and thresholds established by the program prior to convening or reviewing risks.

3.1.9.5. First, establish a core risk assessment team if the program team is not already following a disciplined program acquisition process which incorporates risk assessment activities. This team is the core group of individuals who will conduct the risk assessment and normally includes individuals with expertise in systems engineering, logistics, manufacturing, test, schedule analysis and cost estimating.

3.1.9.6. The risk assessment team should accomplish the following actions:

3.1.9.6.1. Establish the scope of the risk assessment.

3.1.9.6.2. Identify the specific subject-matter experts and arrange for their participation in the risk assessment. The program office needs to ensure it obtains the services of experts in each potential risk area within the program. Subject matter expert time is valuable and limited, therefore grouping topics or focusing their attention on specific and appropriate risks should be considered. It is important to consider outside government organizations for both inputs and team members. They can provide experts and bring different perspectives to the program. Consider such organizations as the using command (both operational and logistics personnel), training organizations, the supporting depot (if identified), test organizations, the laboratories, and the in-plant representative from the Defense Contract Management Agency (DCMA). Non-DoD organizations include the National Aeronautics and Space Administration, the Federal Aviation Administration, and the Department of Energy's national laboratories.

3.1.9.6.3. Prepare a risk assessment training package for the full team (core team plus subject matter experts). This package would include the risk assessment process, analysis criteria, documentation requirements, team ground rules, and a program overview. Bring the full team together for risk assessment training in an integrated manner. The use of a facilitator may be useful to support this training.

3.1.10. After the program's risks have been identified and assessed, the approach to handling each moderate to high risk must be developed. The various risk handling options are analyzed and those best fitted to the program's circumstances selected. These are included in the program's acquisition strategy. Once the acquisition strategy—with the appropriate risk handling approaches —has been defined, the schedule and cost impacts to the basic program schedule and cost estimates must be derived. **Table 3.1** describes a successful assessment of Navy Environment, Safety, and Occupational Health (ESOH) risks, which resulted in a tailored acquisition strategy with significant improvements in program effectiveness and efficiency.

Table 3.1. Example of Successful Program Management of ESOH Risks.

Programmatic ESOH Evaluation (PESHE) Process	
Process:	Incorporating ESOH Analysis into the F/A-18E/F & EA-18G Acquisition Decision Process

Description:	The PESHE served as the Program Manager's (PM) tool for integrating ESOH considerations into all aspects of F/A-18 Programs. The PESHE process identified ESOH risks and strategies to control risk and manage costs, liabilities and schedule for the F-18 Program. Once ESOH concerns are identified, the degree of risk is quantitatively or qualitatively defined based on the consequences and the likelihood of occurrence. The ESOH risk assessment process used Military Standard (MIL-STD) 882C/D and the F/A-18 Risk Management Plan. This approach allowed the Program Office to understand ESOH risks in relation to the overall program risk assessment. Serious, high and medium ESOH risks were included in the overall F/A-18 and EA-18G risk databases. All risks, including ESOH, were reviewed by the Navy led Program Risk Advisory Board (PRAB), comprised of key Program Office, NAVAIR, customer, contractor and supplier representatives. Risk mitigation plans and the status of resolving the risks were part of the PRAB review process. Key ESOH issues and risks were discussed during management meetings and in weekly team notes. ESOH risks (especially high/moderate risks) were addressed during quarterly Green Hornet Team (GHT) meetings. ESOH Manager and GHT members reviewed acquisition program documents (e.g., Initial Capabilities Document, Acquisition Strategy, Test and Evaluation Master Plan, etc.) to incorporate ESOH considerations. ESOH recommendations were submitted for inclusion in the EA-18G Acquisition Strategy, performance specification, and statement of work. ESOH requirements must flow to the subcontractors in all F/A-18 system contracts. The focus was to continue capitalizing on past ESOH efforts to minimize future ESOH risk, relative to new design or upgrade efforts. The GHT proactively reviewed existing and proposed regulations, assessing the potential impact to the F/A-18 program. Efforts were made to reduce and eliminate hazardous material (HAZMAT) use, identify material reduction and recycling opportunities, and implement design changes to reduce ESOH impact and cost.
Benefits/ Savings:	The modified F/A-18E/F reduced adverse ESOH impacts and conserved resources. The new design contained 40% fewer parts and 50% fewer cadmium plated fasteners and reduced production time by 31%. The use of composite skins, which reduced corrosion and maintenance induced damage, extended the aircraft's useful life. Composite skins replaced metal skins that had to be alodined or anodized to reduce the manufacturing and maintenance waste streams, decrease maintenance time, and shrink life-cycle costs. The F/A-18E/F Program reduced HAZMAT use, waste streams, and cost through program management initiatives. The long-term goal was to make the F/A-18 as environmentally friendly as possible without degrading readiness or mission effectiveness.
Source:	FY03 Chief of Naval Operations Environmental Security Awards - F18 ESOH Program

3.2. Summary. Life Cycle Risk Management is everyone's responsibility and a central program management activity, not limited to the Chief Engineer or the office risk manager. It is essential that program managers, engineers, and other functional offices define and implement appropriate risk management and contingency plans early in the process to enhance program effectiveness and reduce life cycle costs. The management of risks starts early in pre-materiel development decision, through materiel solution analysis, and technology development. The process of studying alternatives, building prototypes, and updating the capability requirements build a foundation towards understanding and managing risks associated with engineering and manufacturing development, production and deployment, then finally operations and support.

RUSSELL B. HOWARD, SES, USAF
Director of Engineering and Technical Management

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Major References

AFI 63-101, *Acquisition and Sustainment Life Cycle Management,* Change 2, June 16, 2010

AFI 63-1201, *Life Cycle Systems Engineering*, 23 Jul 2007

AFFARS, *Air Force Supplement to the Federal Acquisition Regulation*

AFMCI 63-1201, *Implementing Operational Safety Suitability & Effectiveness (OSS&E) & Life Cycle Systems Engineering (LCSE),* 14 Oct 09.

AFPAM 63-128, *Guide to Acquisition and Sustainment Life Cycle Management,* October 5, 2009.

Defense Acquisition Guidebook (formerly DOD 5000.2-R)

DoDI 5000.02, *Operation of the Defense Acquisition System,* December 8, 2008.

Federal Acquisition Regulation

MIL-STD-882D, *The DOD Standard Practice for System Safety*, 10 Feb 2000

Risk Management Guide for DoD Acquisition, Sixth Edition, August, 2006

Acronyms

ACAT—Acquisition Category

ACE—Acquisition Center of Excellence

ADM—Acquisition Decision Memorandum

AF—(United States) Air Force

AFFARS—Air Force Federal Acquisition Regulation Supplement

AFI—Air Force Instruction

AFIT—Air Force Institute of Technology

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPAM—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFRL—Air Force Research Laboratory

AoA—Analysis of Alternatives

APB—Acquisition Program Baseline

APML—Acquisition Program Master List

APUC—Average Procurement Unit Cost

ARM—Active Risk Manager

BCA—Business Case Analysis

CBA—Cost Benefit Analysis

CDD—Capability Development Document

CDR—Critical Design Review

CE—Chief Engineer

CF—Consequence of Failure

CJCSI—Chairman, Joint Chiefs of Staff Instruction

COCOM—Constructive Cost Model

CORAM—Consolidated Risk Assessment Methodology

COTS—Commercial-off-the-shelf

CPD—Capability Production Document

CTE—Critical Technology Elements

DAF—Department of the Air Force

DAG—Defense Acquisition Guidebook

DAU—Defense Acquisition University

DBMS—Database Management System

DCMA—Defense Contract Management Agency

DPG—Defense Planning Guidance

DoD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

DRFM—Digital Radio Frequency Memory

EMD—Engineering and Manufacturing Development

ESM—Electronic Warfare Support Measures

ESOH—Environmental, Safety and Occupational Health

EVMS—Earned Value Management System

FAR—Federal Acquisition Regulation

FMECA—Failure Modes, Effects, and Criticality Analysis

FOC—Full Operational Capability

FRP—Full Rate Production

FY—Fiscal Year

GFE—Government Furnished Equipment

GHT—Green Hornet Team

HAZMAT—Hazardous Materials

HMDM—fictitious program name

HWIL—Hardware-in-the-loop

IBR—Integrated Baseline Review

ICD—Initial Capabilities Document

ID—-Identification

IFF—Identification Friend or Foe

IIPT—Integrating IPT

ILCM—Integrated Life Cycle Management

IMP—Integrated Master Plan

IMS—Integrated Master Schedule

IOC—Initial Operational Capability

IPPD—Integrated Product and Process Development

IPT—Integrated Product Team

J&A—Justification and Authorization

JP8—Jet Propellant 8

KDP—Key Decision Point

KPP—Key Performance Parameters

KSA—Key System Attributes

LCC—Life Cycle Costs

LCMP—Life Cycle Management Plan

LCRM—Life Cycle Risk Management

LCSE—Life Cycle Systems Engineering

LRIP—Low Rate Initial Production

LRU—Line Replacement Unit

M&E—Mechanical and Electrical

M&S—Modeling and Simulation

MAJCOM—Major Command

MAJESTIC—fictitious program name

MDA—Milestone Decision Authority

MDAP—Major Defense Acquisition Program

MDD—Materiel Development Decision

MIL-STD—Military Standard

MIS—Management Information System

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MRA—Manufacturing Readiness Assessments

MRAT—Manufacturing Readiness Assessment Tool

MRL—Manufacturing Readiness Level

MS—Milestone

NAVAIR—Naval Air Systems Command

NDI—Non-development Item

OIPT—Overarching IPT

OPR—Office of Primary Responsibility

ORM—Operational Risk Management

OSD—Office Secretary of Defense

OSS&E—Operational Safety, Suitability, and Effectiveness

PAUC—Program Acquisition Unit Cost

PDR—Preliminary Design Review

PESHE—Programmatic Environment, Safety, and Occupational Health

PF—Probability of Failure

PIIPT—Program Integrating Integrated Product Team

PIPT—Program Integrated Product Team

PM—Program Manager

PMD—Program Management Directive

PMWS—Program Manager's Work Station

POC—Point of Contact

PoPS—Probability of Program Success

PRAB—Program Risk Advisory Board

PRR—Production Readiness Review

PSR—Program Support Review

RAR—Risk Assessment Report

RDS—Records Disposition Schedule

REMIS—Reliability and Maintainability Information System

REVIC—Revised Enhanced Intermediate Version of Constructive Cost Model

RFP—Request for Proposal

RI3—Risk Identification: Integration & -Ilities

RIF—Risk Information File

RMIS—Risk Management Information System

RMP—Risk Management Plan

SASET—Software Architecture Sizing and Estimating Tool

SE—Systems Engineering

SEER—System Evaluation and Estimating of Resources

SEP—Systems Engineering Plan

SME—Subject Matter Expert

SPM—System Program Manager

SPML—Sustainment Program Master List

SRR—System Requirements Review

STINFO—Scientific and Technical Information

TD—Technology Development

TPM—Technical Performance Measures

TRA—Technical Readiness Assessment

TRIMS—Technical Risk Identification and Mitigation System

TRL—Technology Readiness Level

WBS—Work Breakdown Structure

WIPT—Working-level IPT

Attachment 2

RISK MANAGEMENT PLAN (RMP) FORMAT

(Extracted from Risk Management Guide for DoD Acquisition, AFI 63-101, and AFPAM 63-128)

A2.1. Preface:

A2.1.1. AFI 63-101 states that "PMs shall pursue a comprehensive integrated risk analysis throughout the life cycle and shall prepare and maintain a risk management plan. Risks include, but are not limited to, cost, schedule, performance, technical, product data access, technology protection, integration, and Environment, Safety, and Occupational Health (ESOH) risks."

A2.1.2. AFMCI 63-1201 states the Chief Engineer (CE) "is a Systems Program Manager (SPM)'s chief technical authority for systems. The CE leads the implementation of a program's systems engineering processes and is accountable to the SPM for ensuring the integrity of those processes, including technical risk assessment focused on ensuring Operational Safety, Suitability, and Effectiveness (OSS&E) of an assigned system." Multi-function or integrated product teams made up of functional representatives (e.g. contracting, finance, safety) have similar responsibilities to the SPM in ensuring effective risk management across the life cycle of the program.

A2.1.3. What follows in **Attachment 2** is a content description, while **Attachment 3** contains a sample RMP that is a compilation of several good risk plans and the results of the DoD Risk Management Working Group Study and recent updates to AF policy. The format and template represent the types of information and considerations that a plan, tailored to a specific program, might contain. The sample in **Attachment 3** is, admittedly, more useful for an ACAT I or II program; however, ACAT III programs may also use it as a guide to write a tailored plan to meet their program needs. The Risk Management Guide for DoD Acquisition contains general guidance and advice in all areas of risk management, which includes some key activities, considerations, and outline. The Air Force has further provided direction in AFI 63-101 and guidance in AFPAM 63-128 to define the steps of the life cycle risk management (LCRM) process and to direct the use of the standardized 5X5 matrix with associated definitions. AFPAM 63-128 also provides many examples and considerations for risk management throughout the life cycle of a program, describing where risk management plays a role at each milestone.

A2.1.4. There is a danger in providing a sample document. First of all, because it is written as a guide for a general audience, it does not satisfy all of the needs of any particular program. Second, there is the possibility that some prospective user will simply adopt the plan as written, despite the fact that it does not fit his or her program. We discourage this.

A2.1.5. The reason for providing this example is to give PMs and their staffs a starting point for their own planning process. It should stimulate thought about what has to be done and give some ideas on how to begin writing a plan. *The sample plan contains more information than most program offices should need*. Few PMs have the resources for a dedicated risk management effort as depicted in the plan. The key to using the sample plan is to *keep things*

simple and tailor the plan to suit your needs, focusing on the management of risk in the *key critical areas of your program.*

A2.2. Content Description for Risk Management Plan:

A2.2.1. ***INTRODUCTION***. *This section should address the purpose and objective of the plan, and provide a brief summary of the program, to include the approach being used to manage the program, and the acquisition strategy.*

A2.2.2. ***PROGRAM SUMMARY.*** *This section contains a brief description of the program, including the acquisition strategy and the program management approach, i.e. how the government manages the program with different stakeholders. The acquisition strategy should address its linkage to the risk management strategy. The program approach should explain how requirements and resources are managed to meet cost, schedule, and performance objectives. The program summary should also briefly cover the existing program structure, i.e. integrated product teams, technical review boards, program review boards, etc.*

A2.2.3. ***DEFINITIONS***. *Definitions used by the program office should be consistent with DoD definitions for ease of understanding and consistency. However, the DoD definitions allow program managers flexibility in constructing their risk management programs. Therefore, each program's risk management plan may include definitions that expand the DoD definitions to fit its particular needs. For example, each plan should include, among other things, the Air Force's standard definitions for the ratings used for technical, schedule, and cost risk.*

A2.2.4. ***RISK MANAGEMENT STRATEGY***. *This section explains the overall risk management strategy and how it integrates with the program management approach. The risk management strategy will state the risk management purpose and objective. The strategy should include the intent to identify root causes and address all risk areas or events that may have a critical impact on the program. The strategy should address both technical and non-technical areas to be evaluated to identify possible risk events that may cause cost, schedule, or performance impacts. Although predictive in nature, the strategy should also address contingency planning when negative events do occur.*

A2.2.5. ***RESPONSIBLE/EXECUTING ORGANIZATION***. *For each risk identified, the program office team must establish how the actual assessment will be conducted. At least four choices are available: conduct the assessment as part of the normal IPT activity of the program office; establish a risk assessment team as a temporary team or permanent organization; establish a government-industry team; or request an outside team or combined program office-outside team*

A2.2.5.1. *This section will assign responsibilities for specific areas and identify additional technical expertise needed. Typically, the program office team is the core group of individuals who will conduct the risk assessment and normally includes individuals with expertise in systems engineering, logistics, manufacturing, test, schedule analysis, and cost estimating. Throughout the duration of each program, assessments will regularly be accomplished (at a minimum, annually) to identify, analyze, and prioritize risk. Risk assessment will be an iterative process conducted throughout the design, development, and sustainment of each system.*

A2.2.6. ***RISK MANAGEMENT PROCESS AND PROCEDURES***. *This section describes the risk management process and areas to consider, which includes delineating considerations for mitigation planning, utilizing the Air Force's rating scheme (AFPAM 63-128), dictating the reporting and documentation needs, and establishing report requirements. The section includes an explanation of the steps to be employed; i.e., risk planning, identification, analysis, mitigation planning, mitigation execution, and tracking and documentation. It should also provide application guidance for each of the risk management functions in the process. If possible, the guidance should be as general as possible to allow the program's risk management organization (e.g., IPTs) flexibility in managing the program risk, yet specific enough to ensure a common and coordinated approach to risk management. It should address how the information associated with each element of the risk management process will be documented and made available to all participants in the process, and how risks will be tracked, to include the identification of specific metrics if possible.*

A2.2.7. ***RISK PLANNING.*** *This section describes the risk planning process and provides guidance on how it will be accomplished, and the relationship between continuous risk planning and the RMP. Guidance on updates of the RMP and the approval process to be followed should also be included. Typically, updates should be considered (1) whenever the acquisition or support strategy changes, or there is a major change in program emphasis; (2) in preparation for major decision points; (3) concurrent with the review and update of other program plans if necessary; (4) from results and findings from event-based technical reviews; (5) in preparation for a Program Objective Memorandum submission.*

A2.2.8. ***RISK IDENTIFICATION.*** *This section of the plan describes the process and procedures for examining the critical risk areas and processes to identify and document the associated risks. The section should provide areas of consideration and explain how to determine the root cause, e.g. decomposing the program to the lower levels of activity or by asking the "5 Why's." This section should also explain how each risk identified will be clearly assigned ownership and responsibility.*

A2.2.9. ***RISK ANALYSIS***. *This section summarizes the analyses process for each of the risk areas leading to the determination of a risk rating. This rating is a reflection of the potential impact of the risk in terms of its variance from known Best Practices or probability of occurrence, its consequence, and its relationship to other risk areas or processes. This section may include an overview and scope of the assessment process; sources of information; information to be reported and formats; description of how risk information is retained; and assessment techniques and tools*

A2.2.9.1. *The objective of this step is to determine the probability that a root cause "X" might occur with the resultant cost/schedule/performance impact "Y". The impact or consequence should be a credible potential result. Optimally, the analysis would be based upon scientific calculations (fault tree analysis) or historic data, but it may have to rely upon expert judgment in many cases. Typically, only the most severe consequence from a root cause is placed on the risk matrix for program reviews. Programs must use the standard Life Cycle Risk Management 5X5 matrix, likelihood criteria and consequence criteria to analyze program risk (ref. AFI 63-101 and AFPAM 63-128). All moderate and high risks must/must be presented using the standard 5X5 matrix as a part of program, technical, and Milestone decision reviews. Mission assurance and system safety risks identified using the MIL-STD-882D will be translated as also described in*

AFI 63-101. Program managers may develop additional consequence criteria if needed, but must describe these in the RMP. The risk analysis must also contain the results of the Failure Modes, Effects, and Criticality Analysis (FMECA) per AFMCI 63-1201. If the likelihood or consequence cannot be reasonably assessed, it may be separately reported as a "concern."

A2.2.10. ***RISK MITIGATION/HANDLING PLANNING.*** *This section explains the process for conducting risk mitigation plans, which describes actions to eliminate or reduce the identified risks, as well as risk measures, indicators, and trigger levels for use in tracking the effectiveness of the mitigation actions.*

A2.2.10.1. *The risk mitigation/handling plans are separately developed from the RMP to address individual risks and are tactical in nature. The defined process should explain how to determine and evaluate various risk mitigation or handling options, and identify tools that can assist in implementing the risk handling process. It should also provide guidance on the use of the various handling options for specific risks. The description of the mitigation/handling options should list all assumptions used in the development of the tasks. Recommended actions that require resources outside the scope of a contract or official tasking should be clearly identified, and the functional areas, the risk category, or other handling plans that may be impacted should be listed.*

A2.2.10.2. *Risk mitigation plans are prepared for all moderate and high risks. Formal decisions to proceed (e.g. Milestone Decisions, Acquisition Strategy Panels, etc.) constitute approval of a program's current risk assessment and mitigation plans. Inherent with this step is developing contingency plans for when the mitigation plans fail.*

A2.2.11. ***RISK MITIGATION/HANDLING IMPLEMENTATION.*** *The intent of risk mitigation (plan) execution is to ensure successful risk mitigation or acceptable handling occurs. It answers the question "How can the planned risk mitigation be implemented?" It determines what planning, budget, requirements and contractual changes are needed; provides a coordination vehicle with management and other stakeholders; directs the teams to execute the defined and approved risk mitigation plans; outlines the risk reporting requirements for on-going monitoring; and documents the change history.*

A2.2.12. ***RISK TRACKING.*** *This section describes the process and procedures that will be followed to execute and monitor the status of the mitigation plan and the various risk events identified. It should provide criteria for the selection of risks to be reported on, and the frequency of reporting. Guidance on the selection of metrics should also be included. The documented information should be focused on supporting event-driven technical reviews to help identify risk areas and the effectiveness of ongoing risk mitigation efforts. Formal decisions to proceed (e.g. Milestone Decisions, Acquisition Strategy Panels, etc.) constitute approval of a program's current risk assessment and mitigation plans. Decisions to implement mitigation actions or acceptance of risks will be documented in program review documentation.*

A2.2.13. ***RISK MANAGEMENT INFORMATION SYSTEM, DOCUMENTATION AND REPORTS.*** *This section describes the MIS structure, rules, and procedures that will be used to document the results of the risk management process. It also identifies the risk management documentation and reports that will be prepared; specifies the format and frequency of the reports; and assigns responsibility for their preparation. Per AFPAM 63-*

128, programs must track all risks and handling/mitigation in a database that archives risk management across each program's life cycle. This is especially important to support the seamless transition of risk management between life cycle phases, responsible organizations, and prime contractors.

A2.2.13.1. *AFMC/EN has available a commercial risk management tool with database capability (Active Risk Manager (ARM)). Prior to expending resources for development or purchase of another risk management tool, contact AFMC/EN to determine this tool's suitability for a specific program. Other less powerful tools, such as probability / consequence cube, may be available at no additional cost as well.*

Attachment 3

SAMPLE RISK MANAGEMENT PLAN

A3.1. INTRODUCTION

A3.1.1. This Risk Management Plan (RMP) presents the process for implementing proactive risk management as part of the overall management of the MAJESTIC program (fictitious program). Risk management is a program management tool to assess and mitigate events that might adversely impact the program thereby increasing the likelihood of success. This RMP will serve as a basis for identifying alternatives to achieve cost, schedule, and performance goals; assist in making decisions on budget and funding priorities; provide risk information for Milestone decisions; and allow risk monitoring as it proceeds.

A3.1.2. The RMP describes methods for identifying, analyzing, prioritizing, and tracking risk drivers; developing risk-handling/mitigation plans; and planning for adequate resources to handle risk. It assigns specific responsibilities for the management of risk and prescribes the documenting, monitoring, and reporting processes to be followed.

A3.1.3. This is the second edition of the Risk Management Plan for the MAJESTIC program. The initial plan concentrated on tasks leading to Milestone B; this plan concentrates on the tasks leading to Milestone C. Subsequent updates to this RMP will shift focus to the later acquisition phases. There are changes in every area of the plan; they include refinement of the risk identification process. The Program Office Risk Management Coordinator has been identified and training of IPT members has commenced.

A3.2. PROGRAM SUMMARY

A3.2.1. The MAJESTIC program was initiated in response to Initial Capabilities Document, (ICD) XXX, dated DD-MM-YYYY and Capability Development Document (CDD), dated DD-MM-YYYY. It is required to support the fundamental objective of U.S. defense policy as stated in Defense Planning Guidance (DPG) and the National Military Strategy. The MAJESTIC system is based on the need for an integrated combat system to link battlefield decision makers. The MAJESTIC mission areas are: (Delineate applicable areas).

A3.2.1.1. The MAJESTIC program will develop and procure 120 advanced platforms to replace the aging HMDM platforms currently in the inventory. In order to meet force structure objectives, the MAJESTIC system must reach Initial Operational Capability (IOC) (four platforms) by FY-19. The program is commencing an eight-year EMD phase that will be followed by a five-year production and deployment phase. The objectives of the EMD phase are to (discuss the specific objectives of this phase). The program has Congressional interest and is restricted to a Research and Development funding ceiling of $300 million.

A3.2.2. **System Description.** The MAJESTIC will be an affordable, yet capable, platform taking advantage of technological simplification and advancements. The MAJESTIC integrated Combat System includes all non-propulsion electronics and weapons. Subsystems provide capabilities in combat control, electronic warfare support measures (ESM), defensive warfare, navigation, radar, interior communications, monitoring, data transfer, tactical support device, exterior communications, and Identification Friend or Foe (IFF). Weapons systems are to be provided by the program offices that are responsible for their development.

The Mechanical and Electrical (M&E) system comprises... The Combat System, M&E systems, and subsystems provide the MAJESTIC system with the capability and connectivity to accomplish the broad range of missions defined in the ICD, CDD, and capability production document (CPD).

A3.2.3. **Acquisition Strategy.** The MAJESTIC program initial strategy is to contract with one prime contractor in Integrated System Design for development of two prototype systems for test and design validation. Due to the technical complexity of achieving the performance levels of the power generation systems, the prime will use two sub-contractors for the engine development and down select to one producer prior to low rate initial production, which is scheduled for FY-18. Various organizations, such as the Air Force Research Laboratory will be funded to provide experts for assessment of specific areas of risk. The program has exit criteria, included in the list in Annex A, that must be met before progressing to the next phase.

A3.2.4. **Program Management Approach**. The MAJESTIC program is managed using the IPPD concept, with program integrated product teams (PIPTs) established largely along the hierarchy of the product work breakdown structure (WBS). There are also cost-performance and test Working IPTs (WIPTs) established for vertical coordination up the chain of command. The PM chairs a program integrating IPT (IIPT) that addresses issues that are not resolved at the WIPT level.

A3.3. DEFINITIONS

A3.3.1. **Risk.** Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan,) as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS). Risk consists of three components. A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring. A probability (or likelihood) assessed at the present time of that future root cause occurring, and the consequence (or effect) of that future occurrence.

A3.3.2. **Risk Event.** Risks and those events within the MAJESTIC program that, if they go wrong, could result in problems in the development, production, and fielding of the system. Risk events should be defined to a level such that the risk and causes are understandable and can be accurately assessed in terms of likelihood/probability and consequence to establish the level of risk. For processes, risk events are assessed in terms of process variance from known best practices and potential consequences of the variance.

A3.3.3. **Technical Risk.** This is the risk associated with the evolution of the design and the production of the MAJESTIC system affecting the level of performance necessary to meet the operational requirements. The contractor's and subcontractors' design, test, and production processes (process risk) influence the technical risk and the nature of the product as depicted in the various levels of the Work Breakdown Structure (product risk).

A3.3.4. **Cost Risk.** This is the risk associated with the ability of the program to achieve its life-cycle cost objectives. Two risk areas bearing on cost are (1) the risk that the cost

estimates and objectives are accurate and reasonable and (2) the risk that program execution will not meet the cost objectives as a result of a failure to mitigate technical risks.

A3.3.5. **Schedule Risk.** These risks are those associated with the adequacy of the time estimated and allocated for the development, production, and fielding of the system. Two risk areas bearing on schedule risk are (1) the risk that the schedule estimates and objectives are realistic and reasonable and (2) the risk that program execution will fall short of the schedule objectives as a result of failure to mitigate technical risks.

A3.3.6. **Risk Ratings.** This is the value that is given to a risk event (or the program overall) based on the analysis of the likelihood/probability and consequences of the event. For the MAJESTIC program, risk ratings of Low, Moderate, or High will be assigned based on the standard guidance from AFI 63-101 and AFPAM 63-128.

A3.3.7. **Independent Risk Assessor.** An independent risk assessor is a person who is not in the management chain or directly involved in performing the tasks being assessed. Use of independent risk assessors is a valid technique to ensure that all risk areas are identified and that the consequence and likelihood/probability (or process variance) are properly understood. The technique can be used at different program levels, e.g., Program Office, Service Field Activities, Contractors, etc. The Program Manager will approve the use of independent assessors, as needed.

A3.3.8. **Templates and Best Practices.** A "template" is a disciplined approach for the application of critical engineering and manufacturing processes that are essential to the success of most programs. The Air Force Manufacturing Readiness Assessment Tool (MRAT) provides a template for assessing manufacturing readiness throughout the acquisition lifecycle. DoD 4245.7-M, *Transition from Development to Production Solving the Risk Equation*, provides a number of broader templates. For each template process described in DoD 4245.7-M, Best Practice Information is described in NAVSO P-6071. These documents outline the ideal or low risk approach and thus serve as a baseline from which risk for some MAJESTIC processes can be assessed.

A3.3.9. **Metrics.** These are measures used to indicate progress or achievement.

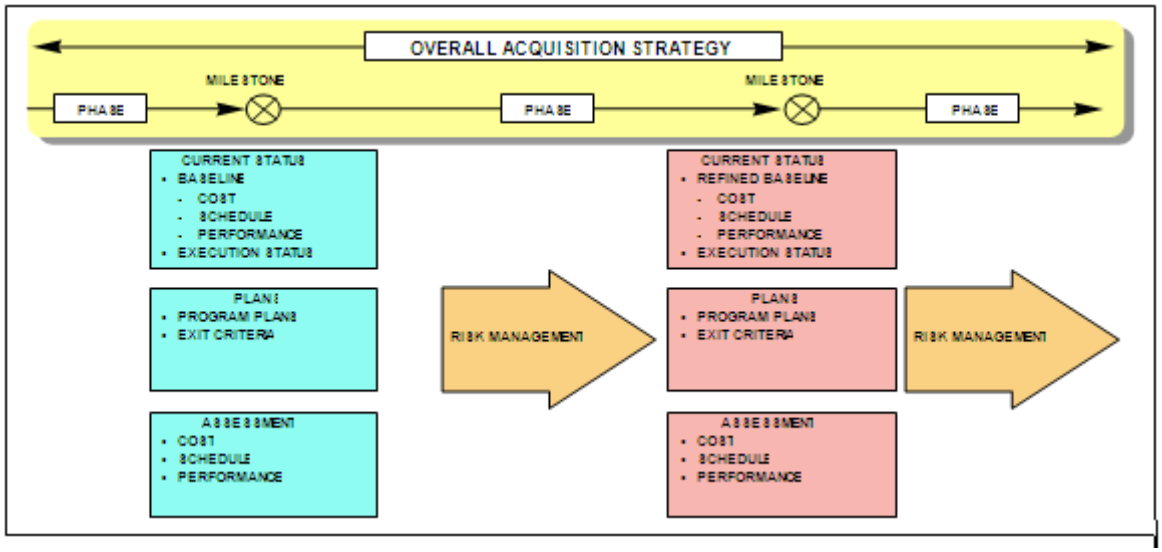
A3.3.10. **Critical Program Attributes.** Critical Program Attributes are performance, cost, and schedule properties or values that are vital to the success of the program. They are derived from various sources, such as the Acquisition Program Baseline, exit criteria for the next program phase, Key Performance Parameters, test plans, the judgment of program experts, etc. The MAJESTIC program will track these attributes to determine the progress in achieving the final required value. See Annex A for a list of the MAJESTIC Critical Program Attributes.

A3.4. RISK MANAGEMENT STRATEGY

A3.4.1. AFI 63-101 identifies the minimum standardized attributes for any Air Force program's risk management effort. Life Cycle Risk Management (LCRM) is the Air Force term for the standardized risk management approach. AFI 63-101 states: "A key element of managing any complex program is the management of risk. PMs on all programs, including commercial-off-the-shelf (COTS) and non-developmental item (NDI) programs must assess and mitigate risks of all kinds as a routine part of program management and must clearly identify risk during program reviews." Furthermore, "PMs shall pursue a comprehensive

integrated risk analysis throughout life cycle and shall prepare and maintain a risk management plan." Per AFMCI 63-1201, the Chief Engineer works closely with the Program Manager to ensure the proper implementation and integrity of a program's Systems Engineering processes, which includes risk management for both technical and non-technical areas.

Figure A3.1. Risk Management and the Acquisition Process.



A3.4.2. The MAJESTIC program will use a centrally developed risk management strategy throughout the acquisition process and decentralized risk planning, assessment, handling, and monitoring. MAJESTIC risk management is applicable to all acquisition functional areas.

A3.4.3. The results of the Materiel Solution Analysis and Technology Development of the program identified potential risk events, and the Acquisition Strategy reflects the program's risk-handling approach. Overall, the risk of the MAJESTIC program for Milestone B was assessed as moderate, but acceptable. Moderate risk functional areas were threat, manufacturing, cost, funding, and schedule. The remaining functional areas of technology, design and engineering (hardware and software), support, (schedule) concurrency, human systems integration, and environmental impact were assessed as low risk.

A3.4.4. The basic risk management strategy is intended to identify critical areas and risk events, both technical and non-technical, and take necessary action to handle them before they can become problems, causing serious cost, schedule, or performance impacts. This program will make extensive use of modeling and simulation, technology demonstrations, and prototype testing to handle risk.

A3.4.5. Risk management will be accomplished using the integrated Government-Contractor IPT organization. These IPTs will use a structured assessment approach to identify and analyze those processes and products that are critical to meeting the program objectives. They will then develop risk-handling/mitigation plans to mitigate the risks and monitor the effectiveness of the selected handling options. Key to the success of the risk management effort is the identification of the resources required to implement the developed risk-handling options.

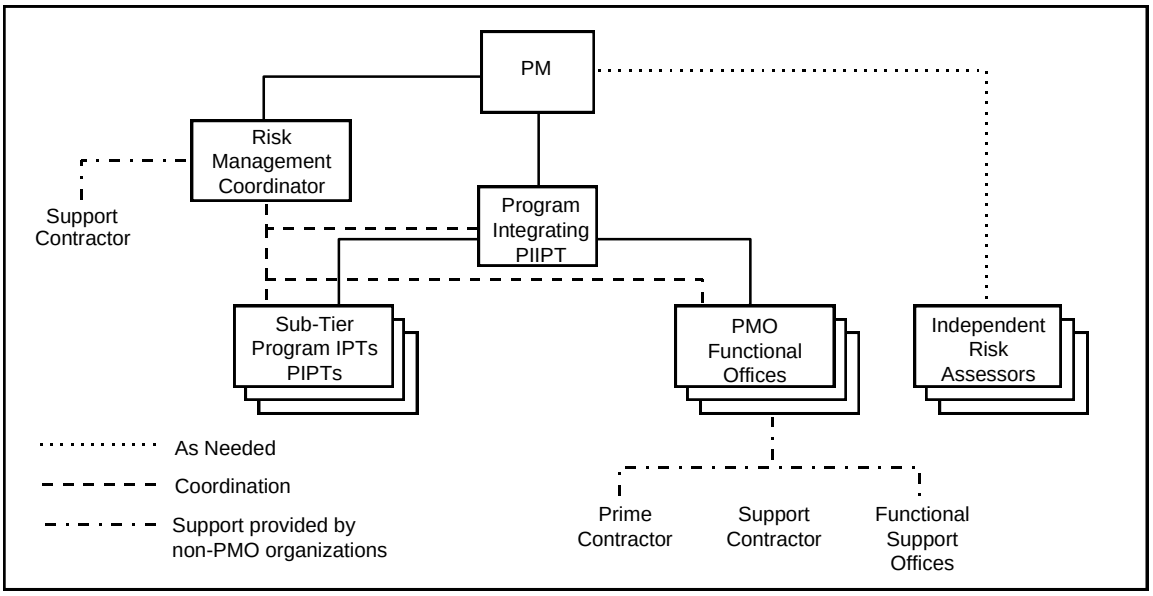
A3.4.6. Risk information will be captured by the IPTs in a risk management information system (RMIS) using a standard Risk Information Form (RIF). The RMIS will provide standard reports, and is capable of preparing ad hoc tailored reports. See Annex D for a description of the RMIS and RIF.

A3.4.7. Risk information will be included in all program reviews, and as new information becomes available, the Program Office and contractor will conduct additional reviews to ascertain if new risks exist. The goal is to be continuously looking to the future for areas that may severely impact the program.

A3.4.8. Risk mitigation efforts have the potential of not being completely successful. In many cases, risk mitigation efforts are not possible (i.e. when risks are accepted). For these types of risks, especially those of high concern, contingency plans will be developed that describe the plan that will be implemented if these risk events occur. Contingency funds and schedule will be set aside to handle these known risk events.

A3.5. RESPONSIBLE/EXECUTING ORGANIZATION. The risk organization for the MAJESTIC program is shown in **Table A3.5.1**. This is *not* a separate organization, but rather shows how risk is integrated into the program's existing organization and shows risk relationships among members of the program team.

Figure A3.5.1. MAJESTIC Risk Management Organization



A3.5.1. **Risk Management Coordinator.** The Risk Management Coordinator, the MAJESTIC Technology Assessment and R&D Manager, is overall coordinator of the Risk Management Program. The Risk Management Coordinator is responsible for:

A3.5.1.1. Maintaining this Risk Management Plan

A3.5.1.2. Maintaining the Risk Management Data Base

A3.5.1.3. Briefing the PM and Chief Engineer on the status of MAJESTIC program risk

A3.5.1.4. Tracking efforts to reduce moderate and high risk to acceptable levels

A3.5.1.5. Providing risk management training

A3.5.1.6. Facilitating risk assessments and

A3.5.1.7. Preparing risk briefings, reports, and documents required for Program Reviews and the acquisition Milestone decision processes.

A3.5.2. **Program Integrating Integrated Product Team (PIIPT).** The PIIPT is responsible for complying with the DoD risk management policy and for structuring an efficient and useful MAJESTIC risk management approach. The Program Manager is the Chair of the PIIPT, with the Chief Engineer as the principle technical and systems engineering risk management advisor. The PIIPT membership may be adjusted but is initially established as the chairs of the Program IPTs, designated sub-tier IPTs, and the Heads of Program Office Functional Offices.

A3.5.3. **PIPTs.** The program IPTs are responsible for implementing risk management tasks per this plan. This includes the following responsibilities:

A3.5.3.1. Review and recommend to the Risk Management Coordinator changes on the overall risk management approach based on lessons learned.

A3.5.3.2. Quarterly, or as directed, update the program risk assessments made during Phase I.

A3.5.3.3. Review and be prepared to justify the risk assessments made and the risk mitigation plans proposed.

A3.5.3.4. Report risk to the Risk Management Coordinator via RIFs.

A3.5.3.5. Ensure that risk is a consideration at each Program and Design Review.

A3.5.3.6. Ensure Design/Build Team responsibilities incorporate appropriate risk management tasks.

A3.5.4. **MAJESTIC Independent Risk Assessors.** Independent Assessors made a significant contribution to the MAJESTIC Milestone B risk assessments. The use of independent assessments as a means of ensuring that all risk areas are identified will continue, when necessary.

A3.5.5. **Other Risk Assessment Responsibilities.** The Risk Assessment responsibilities of other Systems Command codes, Service Field Activities, Design/Build Teams, and Contractors will be as described in Memoranda of Agreement (MOAs), Memoranda of Understanding (MOUs), Systems Command Tasking, or contracts. This RMP should be used as a guide for MAJESTIC risk management efforts.

A3.5.6. **User Participation.** The Requirements Organization (specific code) is the focal point for providing the Program Executive Officer or the Project Manager with user identified risk assessments.

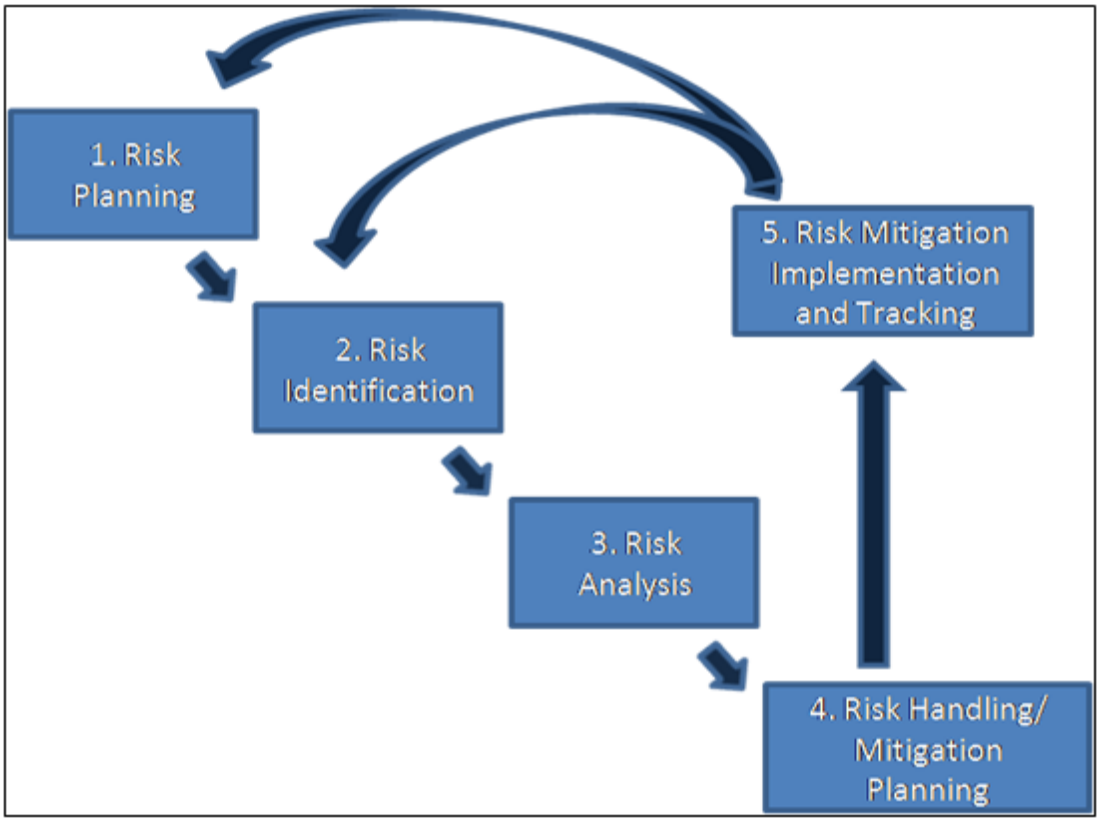
A3.5.7. **Risk Training.** The key to the success of the risk efforts is the degree to which all members of the team both Government and contractors are properly trained. The MAJESTIC Program Office will provide risk training, or assign members to training classes. Key personnel with MAJESTIC management or assessment responsibilities are required to attend. All members of the team will receive, at a minimum, basic risk management training.

MAJESTIC sponsored training is planned to be presented according to the schedule provided in Annex x (not provided).

A3.6. RISK MANAGEMENT PROCESS AND PROCEDURES

A3.6.1. **Overview.** This section describes MAJESTIC program's risk management process and provides an overview of the MAJESTIC risk management approach. Risk Management includes overall planning, identification, analysis, mitigation/tactical planning, plan implementation, and tracking. Tracking addresses the effectiveness of the handling options and the risks themselves to determine how risks have changed. **Table A3.6.1** shows, in general terms, the overall risk management process that will be followed in the MAJESTIC program. This process follows DoD and Service policies and guidelines and incorporates ideas found in other sources. Each of the risk management functions shown in **Table A3.6.1** is discussed in the following paragraphs, along with specific procedures for executing them.

Figure A3.6.1. The Risk Management Process.



A3.6.2. **Risk Planning**

A3.6.2.1. Process. Risk planning consists of the up-front activities necessary to execute a successful risk management program. It is an integral part of normal program planning and management. The planning should address each of the other risk management functions, resulting in an organized and thorough approach to assess, handle, and monitor risks. It should also assign responsibilities for specific risk management actions and

establish risk reporting and documentation requirements. This RMP serves as the basis for all detailed risk planning, which must be continuous.

A3.6.2.2. Procedures

A3.6.2.2.1. Responsibilities. Each IPT is responsible for conducting risk planning, using this RMP as the basis. The planning will cover all aspects of risk management to include identification, analysis, handling/mitigation planning, mitigation implementation, and tracking of risk mitigation activities. The Program Risk Management Coordinator will monitor the planning activities of the IPTs to ensure that they are consistent with this RMP and that appropriate revisions to this plan are made when required to reflect significant changes resulting from the IPT planning efforts.

A3.6.2.2.2. Each person involved in the design, production, operation, support, and eventual disposal of the MAJESTIC system or any of its systems or components is a part of the risk management process. This involvement is continuous and should be considered a part of the normal management process.

A3.6.2.2.3. Resources and Training. An effective risk management program requires resources. As part of its planning process, each IPT will identify the resources required to implement the risk management actions. These resources include time, material, personnel, and cost. Training is a major consideration. All IPT members should receive instruction on the fundamentals of risk management and special training in their area of responsibility, if necessary.

A3.6.2.2.4. Documentation and Reporting. This RMP establishes the basic documentation and reporting requirements for the program. IPTs should identify any additional requirements that might be needed to effectively manage risk at their level. Any such additional requirements must not conflict with the basic requirements in this RMP.

A3.6.2.2.5. Metrics. Each IPT should establish metrics that will measure the effectiveness of their planned risk-handling options. See Annex C for an example of metrics that may be used.

A3.6.2.2.6. Risk Planning Tools. The following tools can be useful in risk planning. It may be useful to provide this information to the contractors to help them understand the MAJESTIC program's approach to managing risk. This list is not meant to be exclusive.

A3.6.2.2.6.1. DoD Manual 4245.7-M, a DoD guide for assessing process technical risk.

A3.6.2.2.6.2. The Navy's Best Practices Manual, NAVSO P-6071, provides additional insight into each of the Templates in DoD 4245.7-M and a checklist for each template.

A3.6.2.2.6.3. Program Manager's Work Station (PMWS) software may be useful to some risk assessors. PMWS has a Risk Assessment module based on the Template Manual and Best Practices Manual.

A3.6.2.2.6.4. Commercial risk management software offer options. Active Risk

Manager (ARM) is one tool that satisfies most/all program requirements.

A3.6.2.2.6.5. Government risk management software, such as *Risk Matrix* developed by MITRE Corporation for the Air Force. The Manufacturing Readiness Assessment Tool (MRAT) is another software tool to help develop a manufacturing maturation plan throughout the acquisition lifecycle.

A3.6.2.2.7. Plan Update. This RMP will be updated, if necessary, on the following occasions: (1) whenever the acquisition strategy changes, or there is a major change in program emphasis; (2) in preparation for major decision points; (3) in preparation for and immediately following technical audits and reviews; (4) concurrent with the review and update of other program plans; and (5) in preparation for a POM submission.

A3.6.3. **Risk Identification and Analysis.** The risk assessment process includes the identification of critical risk events/processes, which could have an adverse impact on the program, and the analyses of these events/processes to determine the likelihood of occurrence/process variance and consequences. It is the most demanding and time-consuming activity in the risk management process.

A3.6.3.1. Process

A3.6.3.1.1. Identification. Risk identification is the first step in the assessment process. The basic process involves searching through the entire MAJESTIC program to determine those critical events that would prevent the program from achieving its objectives. All identified risks will be documented in the RMIS, with a statement of the risk and a description of the conditions or situations causing concern and the context of the risk.

A3.6.3.1.1.1. Risks will be identified by all IPTs and by any individual in the program. The lower-level IPTs can identify significant concerns earlier than otherwise might be the case and identify those events in critical areas that must be dealt with to avoid adverse consequences. Likewise, individuals involved in the detailed and day-to-day technical, cost, and scheduling aspects of the program are most aware of the potential problems (risks) that need to be managed. Each team will determine the root cause for each identified risk, e.g. decomposing the program to the lower levels of activity or by asking the "5 Why's."

A3.6.3.1.2. Analysis. This process involves identification of WBS elements, evaluation of the elements using the risk areas to determine risk events, assignment of likelihood and consequence to each risk event to establish a risk rating, and prioritization of each risk event relative to other risks.

A3.6.3.1.2.1. Risk analysis should be supported by a study, test results, modeling and simulation, trade study, the opinion of a qualified expert (to include justification of his or her judgment), or any other accepted analysis technique. The DoD Acquisition Risk Management Guide describes a number of analysis techniques that may be useful. Evaluators should identify all assumptions made in assessing risk. When appropriate, a sensitivity analysis should be done on assumptions.

A3.6.3.1.2.2. Systems engineering analysis, risk assessments, and manpower risk assessments provide additional information that must be considered. This includes, among other things, environmental impact, system safety and health analysis, and security considerations. Classified programs may experience difficulties in access, facilities, and visitor control that can introduce risk and must be considered.

A3.6.3.1.2.3. The analysis of individual risk will be the responsibility of the IPT identifying the risk, or the IPT to which the risk has been assigned. They may use external resources for assistance, such as field activities, Service laboratories, and contractors. The results of the analysis of all identified risks must be documented in the RMIS.

A3.6.3.2. Procedures

A3.6.3.2.1. Assessments—General. Risk assessment is an iterative process, with each assessment building on the results of previous assessments. The current baseline assessment is a combination of the risk assessment delivered by the contractors as part of the technology development phase, the program office process risk assessment done before Milestone B, and the post-award Integrated Baseline Review (IBR).

A3.6.3.2.1.1. For the program office, unless otherwise directed in individual tasking, program level risk assessments will be presented at each Program Review meeting with a final update not later than 6 months before the next scheduled Milestone decision. The primary source of information for the next assessment will be the current assessment baseline, and existing documentation such as, materiel solution and technology development study results, the design mission profile, the Integrated Baseline Review (IBR), which will be conducted immediately after Milestone B contract award, the contract WBS that is part of the IBR, industry best practices as described in the PMWS Knowledgebase, the CDD, the Acquisition Program Baseline (APB), and any contractor design documents.

A3.6.3.2.1.2. IPTs should continually assess the risks in their areas, reviewing risk-mitigation actions and the critical risk areas whenever necessary to assess progress. For contractors, risk assessment updates should be made as necessary.

A3.6.3.2.1.3. The risk assessment process is intended to be flexible enough so that field activities, service laboratories, and contractors may use their judgment in structuring procedures considered most successful in identifying and analyzing all risk areas.

A3.6.3.2.2. Identification. Following is a description of step-by-step procedures that evaluators may use as a guide to identify program risks.

A3.6.3.2.2.1. **Step One**—Understand the requirements and the program performance goals, which are defined as thresholds and objectives. Describe the operational (functional and environmental) conditions under which the values must be achieved by referring or relating to design documents. The CDD and APB contain Key Performance Parameters (KPPs).

A3.6.3.2.2.2. **Step Two**—Determine the engineering and manufacturing processes that are needed to design, develop, produce, and support the system. Obtain industry best practices for these processes.

A3.6.3.2.2.3. **Step Three**—Identify contract WBS elements (to include products and processes).

A3.6.3.2.2.4. **Step Four**—Evaluate each WBS element against sources/areas of risk described in the DoD Risk Management Guide.

A3.6.3.2.2.5. **Step Five**—Perform a root cause analysis to determine and describe the risk using the "If negative event A occurs, then consequence B will result." Root cause can be determined by using the "5 Why" technique, fault tree analysis, affinity diagram, Pareto, Fishbone, and/or Control Charts.

A3.6.3.2.2.6. IPTs may find the following helpful in identifying and analyzing risk:

A3.6.3.2.2.6.1. **Threat.** The sensitivity of the program to uncertainty in the threat description, the degree to which the system design would have to change if the threat's parameters change, or the vulnerability of the program to foreign intelligence collection efforts (sensitivity to threat countermeasure).

A3.6.3.2.2.6.2. **Requirements.** The sensitivity of the program to uncertainty in the system description and requirements, excluding those caused by threat uncertainty. Requirements include operational needs, attributes, performance and readiness parameters (including KPPs), constraints, technology, design processes, and WBS elements.

A3.6.3.2.2.6.3. **Technical Baseline.** The ability of the system configuration to achieve the program's engineering objectives based on the available technology, design tools, design maturity, etc. Program uncertainties and the processes associated with the "ilities" (reliability, supportability, maintainability, etc.) must be considered. The system configuration is an agreed-to description (an approved and released document or a set of documents) of the attributes of a product, at a point in time, which serves as a basis for defining change.

A3.6.3.2.2.6.4. **Test and Evaluation.** The adequacy and capability of the test and evaluation program to assess attainment of significant performance specifications and determine whether the system is operationally effective, operationally suitable, and interoperable.

A3.6.3.2.2.6.5. **Modeling and Simulation (M&S).** The adequacy and capability of M&S to support all life-cycle phases of a program using verified, validated, and accredited models and simulations.

A3.6.3.2.2.6.6. **Technology.** The degree to which the technology proposed for the program has demonstrated sufficient maturity to be realistically capable of meeting all of the program's objectives.

A3.6.3.2.2.6.7. **Logistics.** The ability of the system configuration and associated documentation to achieve the program's logistics objectives based

on the system design, maintenance concept, support system design, and availability of support data and resources.

A3.6.3.2.2.6.8. **Production/Facilities.** The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources (repair resources in the operations and support phase).

A3.6.3.2.2.6.9. **Concurrency.** The sensitivity of the program to uncertainty resulting from the combining or overlapping of life-cycle phases or activities.

A3.6.3.2.2.6.10. **Industrial Capabilities.** The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system.

A3.6.3.2.2.6.11. **Cost.** The ability of the system to achieve the program's life-cycle support objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined and taking into account known and unknown program information).

A3.6.3.2.2.6.12. **Management.** The degree to which program plans and strategies exist and are realistic and consistent. The government's acquisition and support team should be qualified and sufficiently staffed to manage the program.

A3.6.3.2.2.6.13. **Schedule.** The sufficiency of the time allocated for performing the defined acquisition tasks. This factor includes the effects of programmatic schedule decisions, the inherent errors in schedule estimating, and external physical constraints.

A3.6.3.2.2.6.14. **External Factors.** The availability of government resources external to the program office that are required to support the program such as facilities, resources, personnel, government furnished equipment, etc.

A3.6.3.2.2.6.15. **Budget.** The sensitivity of the program to budget variations and reductions and the resultant program turbulence.

A3.6.3.2.2.6.16. **Earned Value Management System**. The adequacy of the contractor's EVM process and the realism of the integrated baseline for managing the program.

A3.6.3.2.2.6.17. **Failure to Use Best Practices** virtually assures that the program will experience some risk. The further a contractor deviates from best practices, the higher the risk.

A3.6.3.2.2.6.18. **New Processes** should always be suspect, whether they are related to design, analysis, or production. Until they are validated, and until the people who implement them have been trained and have experience in successfully using the process, there is risk.

A3.6.3.2.2.6.19. **Any Process Lacking Rigor** should also be suspect; it is

inherently risky. To have rigor, a process should be mature and documented, it should have been validated, and it should be strictly followed.

A3.6.3.2.2.6.20. **Insufficient Resources:** People, funds, schedule, and tools are necessary ingredients for successfully implementing a process. If any are inadequate, to include the qualifications of the people, there is risk.

A3.6.3.2.2.6.21. **Test Failure** may indicate corrective action is necessary. Some corrective actions may not fit available resources, or the schedule, and (for other reasons as well) may contain risk.

A3.6.3.2.2.6.22. **Qualified Supplier Availability:** A supplier not experienced with the processes for designing and producing a specific product is not a qualified supplier and is a source of risk.

A3.6.3.2.2.6.23. **Negative Trends or Forecasts** are cause for concern (risk) and may require specific actions to turn around.

A3.6.3.2.2.6.24. **Intelligence Supportability.** An intelligence supportability IPT can identify the intelligence data and infrastructure needed to ensure intelligence data is available, supplied, formatted correctly, etc., to support the program.

A3.6.3.2.2.7. There are a number of techniques and tools available for identifying risks. Among them are:

A3.6.3.2.2.7.1. **Active Risk Manager (ARM).** AFMC/EN has available a commercial risk management tool with database capability. Prior to expending resources for development or purchase of another risk management tool, contact AFMC/EN to determine this tool's suitability for a specific program.

A3.6.3.2.2.7.2. **Best Judgment:** The knowledge and experience of the collective, multi-disciplined Integrated Project Team (IPT) members and the opinion of subject matter experts (SMEs) are the most common source of risk identification.

A3.6.3.2.2.7.3. **Lessons Learned** from similar processes can serve as a baseline for the successful way to achieve requirements. If there is a departure from the successful way, there may be risk.

A3.6.3.2.2.7.4. **Risk Identification, Integration, and Ilities Guidebook and Calculator.** Concise set of questions and scoring tool maintained by AFIT/CSE; assists program managers and systems engineers in the development and transition of new technologies by helping them to identify technical risks that have hindered previous programs. Focus areas include 1. People, Organization, Skills; 2. Design Maturity & Stability; 3. Scalability & Complexity; 4. Reliability; 5. Maintainability; 6. Software Development; 7. Human Factors; 8. Integrability; 9. Testability.

A3.6.3.2.2.7.5. **Manufacturing Readiness Assessment Tool (MRAT)** was developed by the Air Force Research Lab, Manufacturing Technology Division, together with the Defense industry to assess the critical factors or

checklist of items that help determine a program's manufacturing readiness to proceed through each acquisition milestone. The tool results in an assessment of the program's manufacturing readiness level and the associated shortfalls that need to be addressed to reduce program risk.

A3.6.3.2.2.7.6. **DoD 4245. 7-M, "Transition from Development to Production,"** is often called the "Templates" book because it identifies technical risk areas and provides, in "bullet" form, suggestions for avoiding those risks. It focuses on the technical details of product design, test, and production to help managers proactively manage risk. It also includes chapters on Facilities, Logistics, and Management, which make this a useful tool in identifying weak areas of MAJESTIC planned processes early enough to implement actions needed to avoid adverse consequences.

A3.6.3.2.2.7.7. **NAVSO P-6071 Best Practices Manual** was developed by the Navy to add depth to the Template Book, DoD 4245.7-M.

A3.6.3.2.2.7.8. **MIL-STD 882D,** Standard Practice for System Safety, is used to identify Environmental, Safety, Occupational Health hazards. These risks will have programmatic impact and need to be translated into the 5X5 matrix as described in **Table A3.6.5**.

A3.6.3.2.2.7.9. **Critical Program Attributes** are metrics that the program office developed to measure progress toward meeting our objectives. Team members, IPTs, functional managers, contractors, etc., may develop their own metrics to support these measurements. The attributes may be specification requirements, contract requirements, or measurable parameters from any agreement or tasking. The idea is to provide a means to measure whether we are on track in achieving our objectives.

A3.6.3.2.2.7.10. **Methods and Metrics for Product Success** is a manual published by the Office of the Assistant Secretary of the Navy (RDA) Product Integrity Directorate. It highlights areas related to design, test, and production processes where problems are most often found and metrics for the measurement of effectiveness of the processes. It also describes the software tool, Program Manager's Work Station (PMWS). See next paragraph.

A3.6.3.2.2.7.11. **PMWS** contains risk management software, "Technical Risk Identification and Mitigation System (TRIMS) and Knowledgebase." They provide a tailorable management system based on NAVSO P-6071 and DoD 4245.7-M. The PMWS provides a compact disk (CD) that contains the necessary programs for assessing a program's risk and software for program management. PMWS can be obtained by calling the Best Manufacturing Program (BMP) Office at (301) 405-9990.

A3.6.3.2.2.7.12. **Risk Matrix** is another candidate for use by the Program Office. It is an automated tool, developed by MITRE Corporation that supports a structured approach for identifying risk and assessing its potential program impact. It is especially helpful for prioritizing risks.

A3.6.3.2.2.7.13. **Requirements Documents** describe the output of our

efforts. IPT efforts need to be monitored continuously to ensure requirements are met on time and within budget. When they aren't, there is risk.

A3.6.3.2.2.7.14. **Contracting for Risk Management** helps ensure the people involved with the details of the technical processes of design, test, and production are involved with managing risk. The principle here is that those performing the technical details are normally the first ones to know when risks exist.

A3.6.3.2.2.7.15. **Quality Standards, such as ISO9000, ANSI/ASQC Q 9000, MIL-HDBK 9000**, and others describe processes for developing and producing quality products. Comparing our processes with these standards can highlight areas we may want to change to avoid risk.

A3.6.3.2.2.7.16. Use of **Independent Risk Assessors** is a method to help ensure all risk is identified. The knowledgeable, experienced people are independent from the management and execution of the processes and procedures being reviewed. Independent assessment promotes questions and observations not otherwise achievable.

A3.6.3.2.2.7.17. Use the **AFMC Intelligence Squadron Acquisition Intelligence Guidebook** to aid in identifying the intelligence supportability needs for the weapons system across the acquisition lifecycle.

A3.6.3.2.3. Analysis. Risk analysis is an evaluation of the identified risk events to determine possible outcomes, critical process variance from known best practices, the likelihood of those events occurring, and the consequences of the outcomes. Once this information has been determined, the risk event may be rated against the Air Force's standardized criteria and an overall assessment of low, moderate, or high assigned. **Tables A3.6.1** through **A3.6.5** depict the risk analysis matrix and standard definitions (ref. AFI 63-101 and AFPAM 63-128).

Table A3.1. Air Force 5X5 Risk Matrix/Rating.

Likelihood					
5	G	Y	R	R	R
4	G	Y	Y	R	R
3	G	G	Y	Y	R
2	G	G	G	Y	Y
1	G	G	G	G	Y
	1	2	3	4	5
	Consequence				

Table A3.6.2. Air Force Probability Criteria.

Level	Likelihood	Probability of Occurrence
1	Not Likely	5-20%
2	Low Likelihood	21-40%
3	Likely	41-60%
4	Highly Likely	61-80%
5	Near Certainty	81-99%

Table A3.6.3. Air Force Consequence Levels.

Level	Technical Performance	Schedule	Cost
1	Minimal consequence to technical performance, but no overall impact to the program success. A successful outcome is not dependent on this issue; the technical performance goals will still be met.	Negligible schedule slip	* A-B Programs: 5% or less increase from MS A approved cost estimate * Post-B & Other Programs: <=1% increase in PAUC or APUC from current baseline estimate, or last approved program cost estimate
2	Minor reduction in technical performance or supportability, can be tolerated with little impact program success. Technical performance will be below the goal or technical design margins will be reduced, but within acceptable limits.	Schedule slip, but able to meet key dates (e.g. PDR, CDR, FRP, FOC) and has no significant impact to slack on critical path	* A-B Programs: >5% to 10% increase from MS A approved cost estimate * Post-B & Other Programs: <=1% increase in PAUC/APUC from current baseline estimate, or last approved program cost estimate, with potential for further cost increase
3	Moderate shortfall in technical performance or supportability with limited impact on program success. Technical performance will be below the goal, but approaching unacceptable limits; or, technical design margins are significantly reduced and jeopardize achieving the system performance threshold values.	Schedule slip that impacts ability to meet key dates (e.g. PDR, CDR, FRP, FOC) and/or significantly decreases slack on critical path	* A-B Programs: >10% to 15% increase from MS A approved cost estimate * Post-B & Other Programs: >1% but <5% increase in PAUC/APUC from current baseline estimate, or last approved program cost estimate
4	Significant degradation in technical performance or major shortfall in supportability with a moderate impact on program success. Technical performance is unacceptably below the goal; or, no technical design margins available and system performance will be below threshold values.	Will require a change to program or project critical path	* A-B Programs: >15% to 20% increase from MS A approved cost estimate * Post-B & Other Programs: 5% but <10% increase in PAUC/ APUC from current baseline estimate, or last approved program cost estimate

5	Severe degradation in technical/ supportability threshold performance; will jeopardize program success; or will cause one of the triggers listed below	Cannot meet key program or project milestones.	* A-B Programs: >20% increase from MS A approved cost estimate * Post-B & Other Programs: >=10% increase in PAUC/APUC from current baseline estimate (danger zone for significant cost growth and Nunn-McCurdy breach), or last approved program cost estimate
Any root cause that, when evaluated by the cross-functional team, has a likelihood of generating one of the following consequences must be rated at Consequence Level 5 in Performance: - Will not meet Key Performance Parameter (KPP) Threshold - Critical Technology Element (CTE) will not be at Technical Readiness level (TRL) 4 at MSKDP A - CTE will not be at TRL 6 at MS/KDP B - CTE will not be at TRL 7 at MS/KDP C - CTE will not be at TRL 8 at the Full-rate Production Decision point - Manufacturing Readiness Level (MRL)* will not be at 8 by MS C - MRL* will not be at 9 by Full-rate Production Decision point - System availability threshold will not be met * MRLs will be calculated in accordance with the DoD Manufacturing Readiness Assessment Deskbook.			

Table A3.6.4. MIL-STD-882D Risk Matrix.

Probability	**A**				
	B				
	C				
	D				
	E				
		IV	**III**	**II**	**I**
	Severity				

Table A3.6.5. Translation of MIL-STD-882D Matrix (Cat I-IV Severity / A-E Probability) to OSD Risk Management Guide 5X5 Matrix.

Likelihood	**5**		**IVA**		**IIA**	**IA**
	4		**IVB**	**IIIA, IIB, IIC**	**IIB**	**IB**
	3		**IVC**	**IIID, IIIE**	**IIC**	**IC**
	2		**IVD**		**IID, IIE**	**ID**

1		**IVE**			**IE**
	1	**2**	**3**	**4**	**5**

Consequence

A3.6.3.2.3.1. Critical Process Variance. For each process risk related event identified, the variance of the process from known standards or best practices must be determined. As shown in **Table A3.6.1**, there are five levels (1-5) in the MAJESTIC risk assessment process. If there is no variance then there is no risk.

A3.6.3.2.3.2. Likelihood/Probability. For each risk area identified, the likelihood the risk will happen must be determined. As shown in **Table A3.6.2**, there are five levels in the MAJESTIC risk assessment process, with the corresponding criteria of *Not Likely, Low Likelihood, Likely, Highly Likely,* and *Near Certainty.* If there is zero likelihood of an event, there is no risk per our definition.

A3.6.3.2.3.3. Consequence. For each risk area identified, the following question must be answered: *Given the event occurs, what is the magnitude of the consequence?* As shown in **Table A3.6.3**, there are five levels of consequence (1-5). "Consequence" is a multifaceted issue. For this program, there are four areas that we will evaluate when determining consequence: technical performance, schedule, cost, and impact on other teams. At least one of the four consequence areas needs to apply for there to be risk; if there is no adverse consequence in any of the areas, there is no risk.

A3.6.3.2.3.3.1. Performance: This category includes all requirements that are not included in the other metrics of the Consequence table. The wording of each level is oriented toward design processes, production processes, operation, life cycle support, and retirement of the system.

A3.6.3.2.3.3.2. Schedule: The words used in the Schedule column, as in all columns of the Consequence table, are meant to be universally applied. Avoid excluding a consequence level from consideration just because it doesn't match your team's specific definitions. In other words, phrases such as need dates, key milestones, critical path, and key team milestones are meant to apply to all IPTs.

A3.6.3.2.3.3.3. Cost: Since costs vary from component to component and process to process, the percentage criteria shown in the table may not strictly apply at the lower levels of the WBS. These team leaders can set the percentage criteria that best reflect their situation. However, when costs are rolled up at higher levels (e.g., Program), the standardized definitions will be used.

A3.6.3.2.3.3.4. Environment, Safety, Occupational Health (ESOH) / MIL-STD-882 hazards: The program manager is required to present ESOH and acquisition risks together at all program reviews, utilizing the DoD 5X5 Risk Matrix. Although ESOH uses a separate management methodology, these

risks need to be translated from the MIL-STD-882D Risk Matrix (**Table A3.6.4**) into the DoD Acquisition 5X5 matrix (**Table A3.6.5**) per AFI 63-101 and AFPAM 63-128. The rationale is that the DoD system safety process employs a unique methodology for mishap risk assessment and prevention. By using the standardized risk assessment and identification processes as outlined in MIL-STD-882D, ESOH risks are identified, controlled, or mitigated and tracked throughout the lifecycle.

A3.6.3.2.3.3.5. Impact on Other Teams: Both the consequence of a risk and the mitigation actions associated with reducing the risk may impact another team. This may involve additional coordination or management attention (resources) and may therefore increase the level of risk. This is especially true of common technical processes.

A3.6.3.2.3.4. Risk Rating. Probability and consequence should not always be considered equally; for example, there may be consequences so severe that it is considered high risk even though the probability to achieve a particular outcome is low. After deciding a level of process variance/likelihood (1 through 5) and a level of consequence (1 through 5), enter the Assessment Guide portion of **Table A3.6.1** to obtain a risk rating (green = LOW, yellow = MOD, and red = HIGH). For example; consequence/process variance/likelihood level 2-2 corresponds to LOW risk, level 3-4 corresponds to MOD risk, and level 4-4 corresponds to HIGH risk. After obtaining the risk rating, make a subjective comparison of the risk event with the applicable rating definition in **Table A3.6.1** (e.g., High=unacceptable, major disruptions, etc.). There should be a close match. If there isn't, consider reevaluating the level of likelihood or consequence. Those risk events that are assessed as moderate or high should be submitted to the MAJESTIC Risk Management Coordinator on a RIF.

A3.6.3.2.3.5. **Table A3.6.1** is useful to convey information to decision makers and will be used primarily for that purpose. The Program Office will use the Risk Tracking Report and Watchlist. (See Annex D.)

A3.6.4. **Risk Handling/Mitigation Planning**

A3.6.4.1. Process. After the program's risks have been identified and assessed, the approach to handling each moderate to high risk must be developed. There are essentially four techniques or options for handling risks: avoidance, control, transfer, and assumption. For all identified risks, the various handling techniques should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, the effect on the system's technical performance, and the most suitable technique selected. The Risk Management Guide for DoD Acquisition contains information on the risk-handling techniques and various actions that can be used to implement them. The results of the evaluation and selection of the risk mitigation plan will be included and documented in the RMIS using the RIF. Contingency plans should also be developed at this time to address the necessary resources when mitigation strategies fail, even though only a portion of these plans will ever be enacted.

A3.6.4.2. Procedures

A3.6.4.2.1. The IPT that assessed the risk is responsible for evaluating and recommending to the PM the risk-handling plans that are best fitted to the program's circumstances. Once approved, these are included in the program's acquisition strategy or management plans, as appropriate.

A3.6.4.2.2. For each selected handling option, the responsible IPT will develop specific tasks that, when implemented, will handle the risk. The task descriptions should explain required actions, the level of effort, and necessary resources. It should also provide a proposed schedule to accomplish the actions including the start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant Program activities/milestones (an example is provided in Annex B), and a cost estimate. The description of the handling options should list all assumptions used in the development of the handling tasks. Assumptions should be included in the RIF. Recommended actions that require resources outside the scope of a contract or official tasking should be clearly identified, and the IPTs, the risk area, or other handling plans that may be impacted should be listed.

A3.6.4.2.3. Reducing requirements as a risk avoidance technique will be used only as a last resort, and then only with the participation and approval of the user's representative.

A3.6.4.2.4. DoD 4245.7-M Templates and NAVSO P-6071 Best Practices are useful in developing risk-handling actions for design, test, or manufacturing process risks.

A3.6.4.2.5. Regarding contingency planning, a Monte Carlo simulation technique that takes into account the probability of occurrence of the risk after mitigation plans have been implemented will be used to develop both cost and schedule reserves for contingency. The reserves are sized based on an 80% confidence level for both cost and schedule. The cost reserve is added to the overall budget of the program and the schedule reserve is added to the project reserve in the integrated schedule.

A3.6.5. **Implementing the Risk Management Plan**

A3.6.5.1. Process. The intent of risk mitigation (plan) execution is to ensure successful risk mitigation or acceptable handling occurs. It answers the question "How can the planned risk mitigation be implemented?" It determines what planning, budget, requirements and contractual changes are needed; provides a coordination vehicle with management and other stakeholders; directs the teams to execute the defined and approved risk mitigation plans; outlines the risk reporting requirements for on-going monitoring, and documents the change history.

A3.6.5.2. Procedures. Executing the risk mitigation plan involves determining: the necessary actions, level of effort, materials required, estimated cost, a proposed schedule. The schedule should show the proposed start date, the time phasing of significant risk reduction activities, the completion date, and the relationship to significant Program activities/milestones (an example is provided in Annex B). The mitigation plans should also include recommended metrics for tracking the action, a list of all assumptions, and the person responsible for implementing and tracking the selected option.

A3.6.6. **Risk Tracking**

A3.6.6.1. Process

A3.6.6.1.1. Risk tracking systematically monitors and evaluates the performance of risk-handling actions. It is part of the Program Office function and responsibility and will not become a separate discipline. Essentially, it compares predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk-handling actions. The effectiveness of the risk-monitoring process depends on the establishment of a management indicator system (metrics) that provides accurate, timely, and relevant risk information in a clear, easily understood manner. (See Annex D.) The metrics selected to monitor program status must 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.

A3.6.6.1.2. To ensure that moderate to high risks are effectively monitored, risk-handling actions (which include specific events, schedules, and "success" criteria) will 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 will be included in the RIF for each identified risk, and thus be resident in the RMIS.

A3.6.6.2. Procedures

A3.6.6.2.1. 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. Each IPT is responsible for monitoring and reporting the effectiveness of the handling actions for the risks assigned. Overall MAJESTIC program risk assessment reports will be prepared by the MAJESTIC Risk Management Coordinator working with the cognizant IPT.

A3.6.6.2.2. Many techniques and tools are available for monitoring the effectiveness of risk-handling actions, and IPTs must ensure that they select those that best suit their needs. No single technique or tool is capable of providing a complete answer—a combination must be used. At a minimum, each IPT will maintain a watchlist of identified high priority risks.

A3.6.6.2.3. Risks rated as Moderate or High risk will be reported to the MAJESTIC Risk Management Coordinator, who will also track them, using information provided by the appropriate IPT, until the risk is considered Low and recommended for "Close Out." The IPT that initially reported the risk retains ownership and cognizance for reporting status and keeping the database current. Ownership means implementing handling plans and providing periodic status of the risk and of the handling plans. Risk will be made an agenda item at each management or design review, providing an opportunity for all concerned to offer suggestions for the best approach to managing risk. Communicating risk increases the program's credibility and allows early actions to minimize adverse consequences.

A3.6.6.2.4. The risk management process is continuous. Information obtained from the monitoring process is fed back for reassessment and evaluations of handling

actions. When a risk area is changed to Low, it is put into a "Historical File" by the Risk Management Coordinator and it is no longer tracked by the MAJESTIC Program Office. The "owners" of all Low risk areas will continue monitoring Low risks to ensure they stay Low.

A3.6.6.2.5. The status of the risks and the effectiveness of the risk-handling actions will be reported to the Risk Management Coordinator:

A3.6.6.2.5.1. Quarterly

A3.6.6.2.5.2. When the IPT determines that the status of the risk area has changed significantly (as a minimum when the risk changes from high to moderate to low, or vice versa)

A3.6.6.2.5.3. When requested by the Program Manager.

A3.7. RISK MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION. The MAJESTIC program will use the Active Risk Manager (ARM) database management system as its RMIS. The system will contain all of the information necessary to satisfy the program documentation and reporting requirements.

A3.7.1. **Risk Management Information System (RMIS)**

A3.7.1.1. The RMIS stores and allows retrieval of risk-related data. It provides data for creating reports and serves as the repository for all current and historical information related to risk. This information will include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The Program Office will use data from the RMIS to create reports for senior management and retrieve data for day-to-day management of the program. The program produces a set of standard reports for periodic reporting and has the ability to create ad hoc reports in response to special queries. See Annex D for a detailed discussion of the RMIS.

A3.7.1.2. Data are entered into the RMIS using the Risk Information Form (RIF). The RIF gives members of the project team, both Government and contractors, a standard format for reporting risk-related information. The RIF should be used when a potential risk event is identified and will be updated as information becomes available as the assessment, handling, and monitoring functions are executed.

A3.7.2. **Risk Documentation.** All program risk management information will be documented, using the RIF as the standard RMIS data entry form. The following paragraphs provide guidance on documentation requirements for the various risk management functions.

A3.7.2.1. Risk-Assessment Documentation. Risk assessments form the basis for many program decisions. From time to time, the PM will need a detailed report of any assessment of a risk event. It is critical that all aspects of the risk management process are documented.

A3.7.2.2. Risk-Handling Documentation. Risk-handling documentation will be used to provide the PM with the information he needs to choose the preferred mitigation option.

A3.7.2.3. Risk-Monitoring Documentation. The PM needs a summary document that tracks the status of high and moderate risks. The Risk Management Coordinator will

produce a risk tracking list that uses information that has been entered from the RMIS. This document will be produced on a monthly basis.

A3.7.3. Reports. Reports are used to convey information to decision-makers and team members on the status of the program and the effectiveness of the risk management program. Every effort will be made to generate reports using the data resident in the RMIS.

A3.7.3.1. Standard Reports. The RMIS will have a set of standard reports. If IPTs or functional managers need additional reports, they should work with the Risk Management Coordinator to create them. Access to the reporting system will be controlled; however, any member of the Government or contractor team may obtain a password to gain access to the information. See Annex E for a description of the MAJESTIC program reports.

A3.7.3.2. Ad Hoc Reports. In addition to standard reports, the Program Office will need to create ad hoc reports in response to special queries. The Risk Management Coordinator will be responsible for these reports.

A3.8. Annex A *(for Sample Risk Management Plan).*

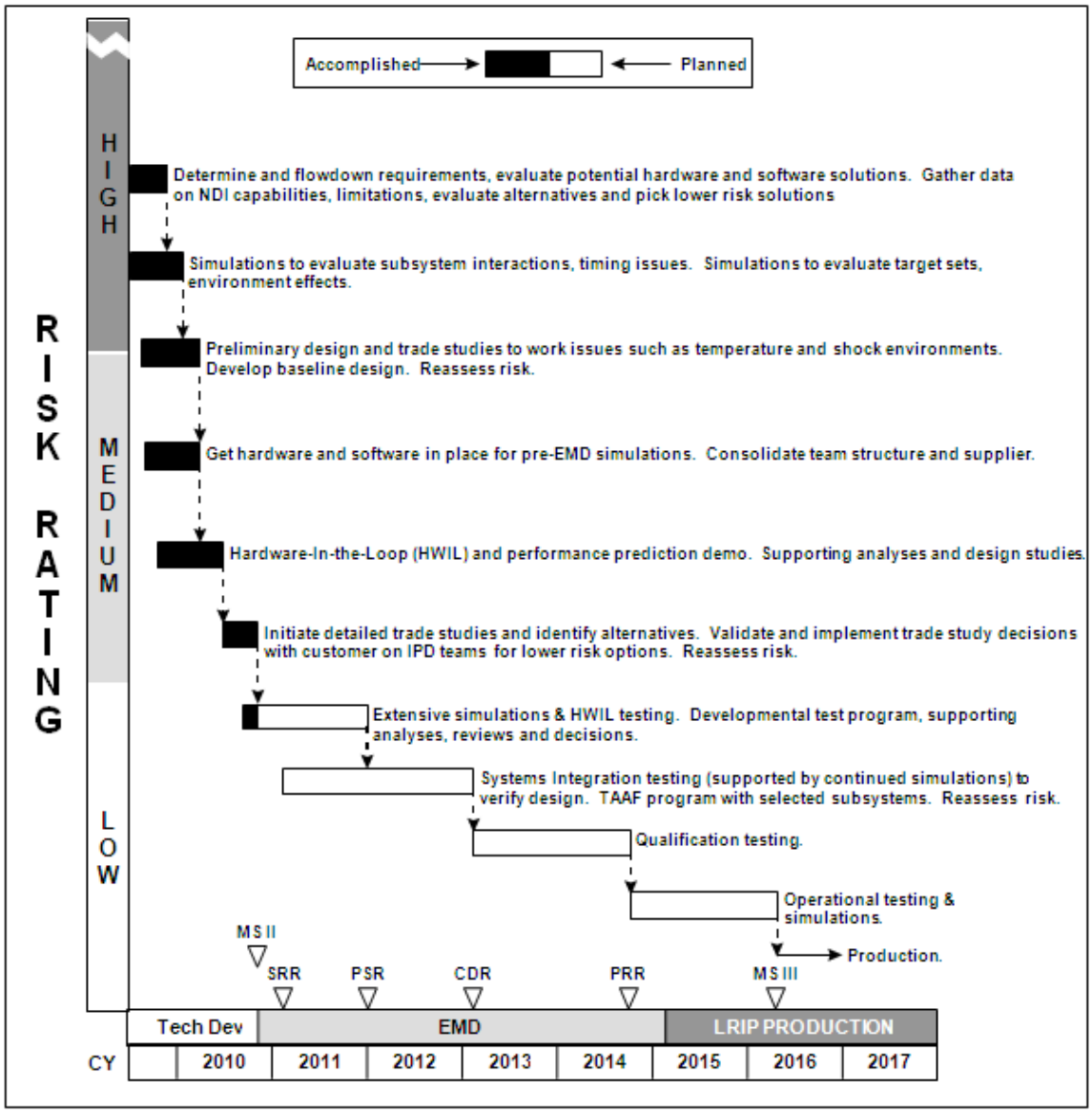
Table A3.8. Critical Program Attributes.

Category	Description	Responsible IPT	Remarks
Performance/Physical	Speed		
	Weight		
	Endurance		
	Crew Size		
	Survivability		
	Maneuverability		
	Size		
	Receiver Range		
	Transmitter Range		
	Data Link Operations		
	Recovery Time		
	Initial Setup		
	Identification Time		
	Accuracy Location		
	Probability of Accurate ID		
	Reliability		
	Maintainability		
	Availability		

	Etc.		
Cost	Operating and Support Costs		
	Etc.		
Processes	Requirements Stable		
	Test Plan Approved		
Exit Criteria	Engine Bench Test		
	Accuracy Verified by Test Data and Analysis		
	Tool proofing Completed		
	Logistics Support Reviewed by User		
	Intelligence Support Reviewed by User		

A3.9. Annex B *(for Sample Risk Management Plan).*

Figure A3.9. Program Risk Reduction Schedule.



A3.10. Annex C (for Sample Risk Management Plan) Program Metric Examples.

Table A3.10.1. Examples of Product-Related Metrics.

Engineering	Requirements	Production	Support

Key Design Parameters Weight Size Endurance Range Design Maturity Open problem reports Number of engineering change proposals Number of drawings released Failure activities Computer Resource Utilization Etc.	Requirements Traceability Requirements Stability Threat Stability Design Mission Profile	Manufacturing Yields Incoming Material Yields Delinquent Requisitions Unit Production Cost Process Proofing Waste Personnel Stability	Special Tools and Test Equipment Requirements Support Infrastructure Footprint Manpower Estimates Support Data Availability (intel)

Table A3.10.2. Examples of Process- Metrics.

Design Requirements	Trade Studies	Design Process	Integrated Test Plan	Failure Reporting System	Manufacturing Plan

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

Table A3.10.3. Examples of Cost and Schedule Metrics.

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

A3.11. Annex D *(for Sample Risk Management Plan)* Management Information System and Documentation.

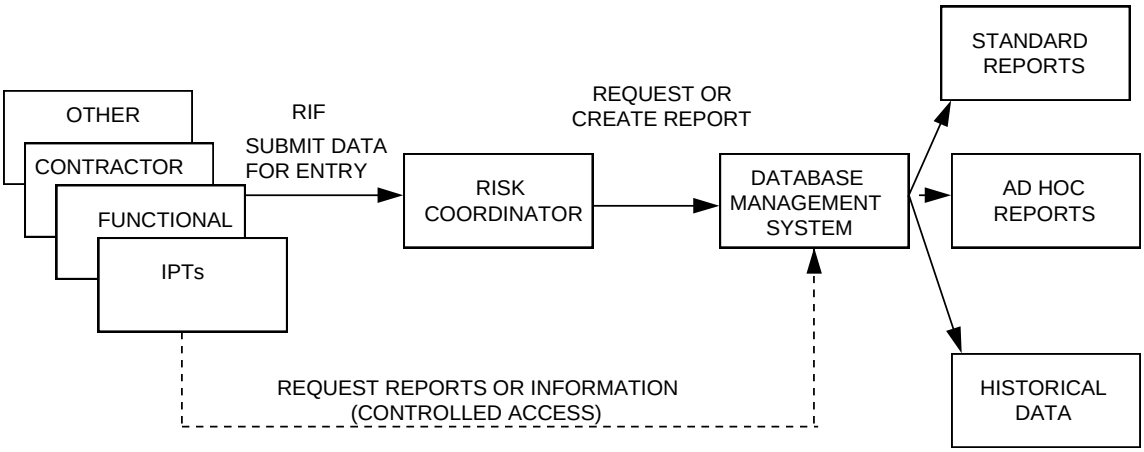
A3.11.1. Description

A3.11.1.1. In order to manage risk, we need a database management system that stores and allows retrieval of risk-related data. The Risk Management Information System provides data for creating reports and serves as the repository for all current and historical information related to risk. This information may include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The Risk Management Coordinator is responsible for the overall maintenance of the RMIS, and he or his designee are the only persons who may enter data into the database.

A3.11.1.2. The RMIS will have a set of standard reports. If IPTs or functional managers need additional reports, they should work with the Risk Management Coordinator to create them. Access to the reporting system will be controlled; however, any member of the Government or contractor team may obtain a password to gain access to the information.

A3.11.1.3. In addition to standard reports, the Program Office will need to create ad hoc reports in response to special queries etc. The Risk Management Coordinator will be responsible for these reports. **Table A3.11.1** shows a concept for a management and reporting system.

Figure A3.11.1. Conceptual Risk Management and Reporting System.



A3.11.2. **Risk Management Reports.** The following are examples of basic reports that a Program Office may use to manage its risk program. Each office should coordinate with the Risk Management Coordinator to tailor and amplify them, if necessary, to meets its specific needs.

A3.11.2.1. Risk Information Form. The Program Office needs a document that serves the dual purpose of a *source* of data entry information and a *report* of basic information for the IPTs, etc. The Risk Information Form (RIF) serves this purpose. It gives members of the project team, both Government and contractors, a format for reporting risk-related information. The RIF should be used when a potential risk event is identified and updated over time as information becomes available and the status changes. As a source of data entry, the RIF allows the database administrator to control entries. The format for a RIF is included after paragraph 3.

A3.11.2.2. Risk Assessment Report. Risk assessments form the basis for many program decisions, and the PM may need a detailed report of assessments of a risk event that has been done. A Risk Assessment Report (RAR) is prepared by the team that assessed a risk event and amplifies the information in the RIF. It documents the identification, analysis, and handling processes and results. The RAR amplifies the summary contained in the RIF, is the basis for developing risk-handling plans, and serves as a historical recording of program risk assessment. Since RARs may be large documents, they may be stored as files. RARs should include information that links it to the appropriate RIF.

A3.11.2.3. Risk-Handling Documentation. Risk-handling documentation may be used to provide the PM with information he needs to choose the preferred mitigation option and is the basis for the handling plan summary contained in the RIF. This document describes the examination process for risk-handling options and gives the basis for the selection of the recommended choice. After the PM chooses an option, the rationale for that choice may be included. There should be a time-phased plan for each risk-mitigation task. Risk-handling plans are based on results of the risk assessment. This document should include information that links it to the appropriate RIF.

A3.11.2.4. Risk Monitoring Documentation. The PM needs a summary document that tracks the status of high and moderate risks. The MAJESTIC program will use a risk-tracking list that contains information that has been entered from the RIF.

A3.11.3. **Database Management System (DBMS)**

A3.11.3.1. The MAJESTIC Risk Management Information System (RMIS) provides the means to enter and access data, control access, and create reports.

A3.11.3.2. Key to the MIS is the data elements that reside in the database. Listed below are the types of risk information that will be included in the database. "Element" is the title of the database field; "Description" is a summary of the field contents. The Risk Management Coordinator will create the standard reports such as, the RIF, Risk Monitoring, etc. The RMIS also has the ability to create "ad hoc" reports, which can be designed by users and the Risk Management Coordinator.

Table A3.11. DBMS Elements.

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the Program Office. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the Program Office compared to all other risks, e.g., a one indicates the highest priority.
Date Submitted	Gives the date that the RIF was submitted.
Major System/ Component	Identifies the major system/component based on the Work Breakdown Structure (WBS).
Subsystem/ Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) of the risk.

Description of Risk	Briefly describes the risk; lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, include how it is manifested (e.g., design and engineering, manufacturing, etc.
Key parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report (see next paragraph), if appropriate.
Analysis	Briefly describes the analysis done to assess the risk; includes rationale and basis for results
Process Variance	States the variance of critical technical processes from known standards or best practices, based on definitions in the program's risk management plan.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's risk-management plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the program's risk-management plan.
Time Sensitivity	Estimates the relative urgency for implementing the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measurement and metrics for tracking progress in implementing risk-handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk-handling milestones.
Status Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

A3.12. Annex E *(for Sample Risk Management Plan)* Example Risk Monitoring Forms.

Figure A3.12.1. Risk Information Form

Risk Information Form

Risk Identification Number Date
Risk Event:
Priority

Major System/ Component/Functional Area:

Category:

Statement of Risk:
Description of Risk:

Key parameters:
Assessment:

Analysis:

Process Variance
Probability of Occurrence:
Consequence:

Time Sensitivity:
Other Affected Areas:

Risk Handling Plans:

Risk Monitoring Activity:

Status: Status Date:

Assignment: Reported By

Figure A3.12.2. Example Risk Tracking Report.

Risk Area Status: Design P_F Hi C_F: Hi

Significant Design Risks:

1. Title: System Weight P_F Hi C_F: Hi

Risk: If advanced composite design fails durability tests, then alternate material will increase system weight by 10%; decreasing the range and increasing fuel consumption.

Action: Examining sub-systems to determine areas where weight may be reduced. Reviewing the durability requirement. Closely watching the effect on reliability and survivability.

2. Title: Design Analysis P_V: Hi C_V: Hi

Risk: If Failure Modes, Effects and Criticality Analysis (FMECA) is completed 2 weeks late, then program will fail to identify and correct any critical single point failure points prior to design freeze.

Action: Additional resources are being sought to expedite performance of FMECA.

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

1. Title: Operational Support P_F Hi C_F: Mod/Hi

Risk: If power supply sub-contractor goes out of business, then no other known sources exist.

Action: Doing trade study to see if alternative designs have a broader power supply vendor base. Prime contractor is negotiating with the sub-contractor to buy drawings for development of second source.

Table A3.12.1. Example Watchlist.

Potential Risk Event	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
Accurately predicting shock environment equipment will experience.	Use multiple finite element codes & simplified numerical models for early assessments. Shock test simple isolated structure, simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SE03 SE03	31 Aug 10 31 Aug 10		

□Evaluating acoustic impact of ship systems that are not similar to previous designs.	□Concentrate on acoustic modeling and scale testing of technologies not demonstrated successfully in large scale tests or full scale trials. □Factor acoustic signature mitigation from isolated modular decks into system requirements. Continue model tests to validate predictions for isolated decks.	SE031 SE032	31 Aug 10 31 Aug 10		

Table A3.12.2. Standard reports from ARM Reporting Services

The ARM program automatically creates the following reports:

List/Data Reports	Analysis Reports	Administrative Reports
Risk Register	PID	Resource Register
Risk Detail	Risk Metrics Summary	Resource Detail
Risk List with Responses	Risk Metrics	User Access/Audit Log
Summary Detail	Risk Heat Map	System usage
Response Register	Risk Staleness	Report Usage
Response Detail	Total Risk List	Scoring Schemes
Evaluation Report	Impact Probability	Role Rights
Incident Report	Analysis	System Security
Loss Register	Impact Cost Chart	System Preferences
Loss Detail	Dashboard	System Maintenance
Accident Register	Corporate Report	System Integration
Accident Detail	Risk Performance Report	System Configuration
Full Risk Data Dump	Risk Process Report	System Filters
Item Register	Risk Process Health	Alert Management
Item Detail	Risk Tracker	Configuration
Item Browser	Losses Summary	
	Return On Investment	
	Trend	

Table A3.12.3. Available Crystal Reports from ARM.

Management Reports	Metric Reports	Administrative Reports

Breakdown of Impacts by Ownership Business Analysis Data Sheet Detailed Register Evaluation Tests Impact Category Summary Index List Performance Against Individual Response Owners Qualitative Impact Record Qualitative Register Qualitative Summary Quantitative Register Report Against Business Structure Response Effectiveness Register Response Evaluation Register Scoring Schemes Severity By Status Summary Detail Relationships	Impact Snapshot Chart Impact Trend Chart Increased and Decreased Impacts Chart New and Changed Risks, Issues, etc Chart New Risks, Issues, etc. Chart Score Changes Report Status Changes Chart Status Changes Report	Database Schema Folder Access List Risk, Issue etc. Access List User Groups and their Users User register Users and their User Groups